maximum use of DoD Component resources and systems established to implement 32 CFR part 285.

(c) The *Head of each DoD Component* shall:

(1) Designate a senior official who shall be responsible for the direction and administration of the Component's Information Security Program, to include active oversight, and security education and training programs to ensure implementation of DoD 5200.1–R within the Component.

(2) Ensure that funding and resources are adequate to carry out such oversight, and security education and training programs.

(3) Consider and take action on complaints and suggestions from persons within or outside the government regarding the Component's Information Security Program.

(4) Establish procedures to limit access to classified information to those who need to know.

(5) Develop plans for the protection, removal, or destruction of classified material in case of fire, natural disaster, civil disturbance, terrorist activities, or enemy action. These plans shall include the treatment of classified information located in foreign countries.

(d) Pursuant to E.O. 12356, the *Director, National Security Agency/Chief, Central Security Service,* as the designee of the Secretary of Defense, is authorized to impose special requirements with respect to the marking, reproduction, distribution, accounting, and protection of and access to classified cryptologic information. The Director, National Security Agency/Chief, Central Security Service, will develop special procedures for the declassification review of cryptologic information. This authority may not be redelegated.

PART 159a—INFORMATION SECURITY PROGRAM REGULATION

Subpart A—Policy

Subpart B—General Provisions

Subpart C—Classification

Subpart D—Declassification and Downgrading

Subpart E—Marking

Subpart F—Safekeeping and Storage

Subpart G—Compromise of Classified Information

AUTHORITY: E.O. 12356, 5 U.S.C. 301.

SOURCE: 54 FR 26959, June 27, 1989, unless otherwise noted.

Subpart A—Policy

§ 159a.1 Purpose.

Information of the Department of Defense relating to national security shall be protected against unauthorized disclosure as long as required by national security considerations. This part establishes a system for classification, downgrading and declassification of information; sets forth policies and procedures to safeguard such information; and provides for oversight and administrative sanctions for violations.

§ 159a.2 Applicability.

This part governs the DoD Information Security Program and takes precedence over all DoD Component regulations that implement that Program. Under 32 CFR part 159, E.O. 12356, and Information Security Oversight Office (ISOO) Directive No. 1, it establishes, for the Department of Defense, uniform policies, standards, criteria, and procedures for the security classification, downgrading, declassification, and

safeguarding of information that is owned by, produced for or by, or under the control of the Department of Defense or its Components.

§ 159a.3 Nongovernment operations.

Except as otherwise provided herein, the provisions of this part that are relevant to operations of nongovernment personnel entrusted with classified information shall be made applicable thereto by contracts or other legally binding instruments. (See DOD Directive 5220.22[1], DoD 5220.22–R[2], and DoD 5220.22–M[3].

§ 159a.4 Combat operations.

The provisions of this part relating to accountability, dissemination, transmission, or safeguarding of classified information may be modified by military commanders but only to the extent necessary to meet local conditions in connection with combat or combat-related operations. Classified information should be introduced into forward combat areas or zones or areas of potential hostile activity only when essential to accomplish the military mission.

§ 159a.5 Atomic energy material.

Nothing in this part supersedes any requirement related to ''Restricted Data'' in the Atomic Energy Act of August 30, 1954, as amended, or the regulations of the Department of Energy under that Act. ''Restricted Data'' and material designated as ''Formerly Restricted Data,'' shall be handled, protected, classified, downgraded, and declassified to conform with Pub. L. 83–703 and the regulations issued pursuant thereto.

§ 159a.6 Sensitive compartmented and communications security information.

(a) Sensitive Compartmented Information (SCI) and Communications Security (COMSEC) Information shall be handled and controlled in accordance with applicable national directives and DOD Directives and Instructions. Other classified information, while in established SCI or COMSEC areas, may be handled in the same manner as SCI or COMSEC information. Classification principles and procedures, markings, downgrading, and declassification actions prescribed in this part apply to SCI and COMSEC information.

(b) Pursuant to 32 CFR part 159, the Director, National Security Agency/Chief, Central Security Service may prescribe special rules and procedures for the handling, reporting of loss, storage, and access to classified communications security devices, equipments, and materials in mobile, handheld or transportable systems, or that are used in conjunction with commercial telephone systems, or in similar circumstances where operational demands preclude the application of standard safeguards. These special rules may include procedures for safeguarding such devices and materials, and penalties for the negligent loss of government property.

§ 159a.7 Automatic Data Processing systems.

This part applies to protection of classified information processed, stored or used in, or communicated, displayed or disseminated by an automatic data processing (ADP) system. Additional security policy, responsibilities, and requirements applicable specifically to ADP systems are contained in DoD Directive 5200.28[4] and DoD 5200.28–M.

Subpart B—General Provisions

§ 159a.9 Definitions.

(a) *Access.* The ability and opportunity to obtain knowledge of classified information.

(b) *Applicable Associated Markings.* The markings, other than classfication markings, and warning notices listed or refered to in § 159a.31(d).

(c) *Carve-Out.* A classified contract issued in connection with an approved Special Access Program in which the Defense Investigative Service has been

[1] Copies may be obtained, if needed, from the Naval Publications and Forms Center, Attn: Code 106, 5801 Tabor Avenue, Philadelphia, PA 19120.

[2] Copies may be obtained at cost, from the National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161.

[3] Copies may be obtained, at cost, from the Government Printing Office.

[4] See footnote 1 to § 159a.3.

relieved of inspection, responsibility in whole or in part under the Defense Industrial Security Program.

(d) *Classification Authority.* The authority vested in an official of the Department of Defense to make an initial determination that information requires protection against unauthorized disclosure in the interest of national security.

(e) *Classification Guide.* A document issued by an authorized original classifier that prescribes the level of classification and appropriate declassification instructions for specified information to be classified derivatively. For purposes of this part, this term does not include DD Form 254, ''Contract Security Classification Specification.''

(f) *Classified Information.* Information or material that is:

(1) Owned by, produced for or by, or under the control of the U.S. Government; and

(2) Determined under E.O. 12356 or prior orders and this part to require protection against unauthorized disclosure; and

(3) So designated.

(g) *Classifier.* An individual who makes a classification determination and applies a security classification to information or material. A classifier may be an original classification authority or a person who derivatively assigns a security classification based on a property classified source or a classification guide.

(h) *Communications Security (COMSEC).* The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications and to ensure the authenticity of such communications. COMSEC includes cryptosecurity, emission security, transmission security, and physical security of COSMEC material and information.

(i) *Compromise.* The disclosure of classified information to persons not authorized access thereto.

(j) *Confidential Source.* Any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation, expressed or implied, that the information or relationship, or both, be held in confidence.

(k) *Continental United States (CONUS).* United States territory, including adjacent territorial waters, located within the North American continent between Canada and Mexico.

(l) *Controlled Cryptographic Item (CCI).* A secure telecommunications or information handling equipment ancillary device, or associated cryptographic component, which is unclassified but controlled.

NOTE: Equipments and components so designated bear the designator ''Controlled Cryptographic Item'' or ''CCI.'')

(m) *Critical Nuclear Weapon Design Information.* That Top Secret Restricted Data or Secret Restricted Data revealing the theory of operation or design of the components of a thermo-nuclear or implosion-type fission bomb, warhead, demolition munition or test device. Specifically excluded is information concerning arming, fuzing, and firing systems; limited life components; and total contained quantities of fissionable, fusionable, and high explosive materials by type. Among these excluded items are the components which DoD personnel set, maintain, operate, test, or replace.

(n) *Custodian.* An individual who has possession of or is otherwise charged with the responsibility for safeguarding or accounting for classified information.

(o) *Declassification.* The determination that classified information no longer requires, in the interest of national security, any degree of protection against unauthorized disclosure, together with a removal or cancellation of the classification designation.

(p) *Declassification Event.* An event that eliminates the need for continued classification of information.

(q) *Derivative Classification.* A determination that information is in substance the same as information currently classified, and the application of the classification markings.

(r) *Document.* Any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed matter, data processing cards and tapes, maps, charts, paintings, drawings,

engravings, sketches, working notes and papers, or reproductions by any means or process, and sound, voice, magnetic or electronic recordings in any form.

(s) *DoD Component*. The Office of the Secretary of Defense (OSD), the Military Departments, the Organization of the Joint Chiefs of Staff (OJCS), the Unified and Specified Commands, and the Defense Agencies.

(t) *Downgrade*. A determination that classified information requires, in the interest of national security, a lower degree of protection against unauthorized disclosure than currently provided, together with a changing of the classification designation to reflect such lower degree of protection.

(u) *Foreign Government Information*. Information that is:

(1) Provided to the United States by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or

(2) Produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence.

(v) *Formerly Restricted Data*. Information removed from the Restricted Data category upon a joint determination by the Department of Energy (or antecedent agencies) and the Department of Defense that such information relates primarily to the military utilization of atomic weapons and that such information can be safeguarded adequately as classified defense information. For purposes of foreign dissemination, however, such information is treated in the same manner as Restricted Data.

(w) *Information*. Knowledge that can be communicated by any means.

(x) *Information Security*. The result of any system of policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, information whose protection is authorized by executive order or statute.

(y) *Intelligence Activity*. An activity that an agency within the Intelligence Community is authorized to conduct under E.O. 12333.

(z) *Limited Dissemination*. Restrictive controls for classified information established by an original classification authority to emphasize need-to-know protective measures available within the regular security system.

(aa) *Material*. Any product or substance on, or in which, information is embodied.

(bb) *National Security*. The national defense and foreign relations of the United States.

(cc) *Need-to-know*. A determination made by a possessor of classified information that a prospective recipient, in the interest of national security, has a requirement for access to, or knowledge, or possession of the classified information in order to accomplish lawful and authorized Government purposes.

(dd) *Original Classification*. An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure, together with a classification designation signifying the level of protection required.

(ee) *Regrade*. A determination that classified information requires a different degree of protection against unauthorized disclosure than currently provided, together with a change of classification designation that reflects such different degree of protection.

(ff) *Restricted Data*. All data concerning:

(1) Design, manufacture or utilization of atomic weapons;

(2) The production of special nuclear material; or

(3) The use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category under section 142 of Pub. L. 83–703.

(gg) *Security Clearance*. A determination that a person is eligible under the standards of DoD 5200.2–R for access to classified information.

(hh) *Senior Information Security Authority*. A senior official designated in

writing by the head of each DoD Component to be responsible for implementation of the Information Security Program within the Component.

(ii) *Sensitive Compartmented Information*. Information and material that requires special controls for restricted handling within compartmented intelligence systems and for which compartmentation is established.

(jj) *Special Access Program*. Any program approved in accordance with subpart M of this part which imposes need-to-know or access controls beyond those normally required for access to Confidential, Secret, or Top Secret information.

(kk) *Special Activity*. An activity, or functions in support of such activity, conducted in support of national foreign policy objectives abroad that is planned and executed so that the role of the U.S. Government is neither apparent nor acknowledged publicly; but that is not intended to influence U.S. political processes, public opinion, policies, or media, and does not include diplomatic activities or the collection and production of intelligence or related support functions.

(ll) *Unauthorized Disclosure*. A communication or physical transfer of classified information to an unauthorized recipient.

(mm) *United States and Its Territories, Possessions, Administrative, and Commonwealth Areas*. The 50 States; the District of Columbia; the Commonwealth of Puerto Rico; the Territories of Guam, American Samoa, and the Virgin Islands; the Trust Territory of the Pacific Islands; and the Possessions, Midway and Wake Islands.

(nn) *Upgrade*. A determination that certain classified information requires, in the interest of national security, a higher degree of protection against unauthorized disclosure than currently provided, together with a changing of the classification designation to reflect such higher degree.

§ 159a.10 Policies.

(a) *Classification*—(1) *Basic Policy*. Except as provided in the Atomic Energy Act of 1954, as amended, E.O. 12356, as implemented by the ISOO Directive No. 1, and this part, provides the only basis for classifying information. It is the policy of the Department of Defense to make available to the public as much information concerning its activities as possible consistent with the need to protect the national security. Accordingly, security classification shall be applied only to protect the national security.

(2) *Resolution of Doubts*. Unnecessary classification and higher than necessary classification should be avoided. If there is reasonable doubt about the need to classify information, it shall be safeguarded as if it were classsified ''Confidential'' pending a determination by an original classification authority, who shall make this determination within 30 days. If there is reasonable doubt about the appropriate level of classification, it shall be safeguarded at the higher level of classification pending a determination by an original classification authority, who shall make this determination within 30 days. Upon a classification determination, markings shall be applied in accordance with subpart E of this part.

(3) *Duration*. Information shall be classified as long as required by national security considerations. Each decision to classify requires a simultaneous determination of the duration such classification must remain in force or that the duration of classification cannot be determined.

(b) *Declassification*. Decisions concerning declassification shall be based on the loss of the information's sensitivity with the passage of time or upon the occurrence of a declassification event.

(c) *Safeguarding*. Information classified under this part shall be afforded the level of protection against unauthorized disclosure commensurate with the level of classification assigned under the varying conditions that may arise in connection with its use, dissemination, storage, movement or transmission, and destruction.

§ 159a.11 Security classification designations.

(a) *General*. Information or material that requires protection against unauthorized disclosure in the interest of national security shall be classified in one of three designations, namely:

''Top Secret,'' ''Secret,'' or ''Confidential.'' The markings ''For Official Use Only,'' and ''Limited Official Use'' shall not be used to identify classified information. Moreover, no other term such as ''Sensitive,'' ''Conference,'' or ''Agency'' shall be used in conjunction with the authorized classification designations to identify classified information.

(b) *Top Secret.* ''Top Secret'' shall be applied only to information or material the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security. Examples of exceptionally grave damage include armed hostilities against the United States or its allies; disruption of foreign relations vitally affecting the national security; the compromise of vital national defense plans or complex cryptologic and communications intelligence systems; the revelation of sensitive intelligence operations; and the disclosure of scientific or technological developments vital to national security.

(c) *Secret.* ''Secret'' shall be applied only to information or material the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security. Examples of serious damage include disruption of foreign relations significantly affecting the national security; significant impairment of a program or policy directly related to the national security; revelation of significant military plans or intelligence operations; compromise of significant military plans or intelligence operations; and compromise of significant scientific or technological developments relating to national security.

(d) *Confidential.* ''Confidential'' shall be applied only to information or material the unauthorized disclosure of which reasonably could be expected to cause damage to the national security. Examples of damage include the compromise of information that indicates strength of ground, air, and naval forces in the United States and overseas areas; disclosure of technical information used for training, maintenance, and inspection of classified munitions of war; revelation of performance characteristics, test data, design, and production data on munitions of war.

§ 159a.12 Authority to classify, downgrade, and declassify.

(a) *Original Classification Authority*—(1) *Control.* Authority for original classification of information as Top Secret, Secret, or Confidential may be exercised only by the Secretary of Defense, the Secretaries of the Military Departments, and by officials to whom such authority is specifically delegated in accordance with and subject to the restrictions of this section of the part. In the absence of an original classification authority, the person designated to act in his or her absence may exercise the classifier's authority.

(2) *Delegation of Classification Authority.* Original classification authority shall not be delegated to persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide. Delegations of original classification authority shall be limited to the minimum number required for efficient administration and to those officials whose duties involve the origination and evaluation of information warranting classification at the level stated in the delegation.

(i) *Top Secret.* Only the Secretary of Defense, the Secretaries of the Military Departments, and the senior official designated by each under §5.3(a) of E.O. 12356, provided that official has original Top Secret classification authority, may delegate original Top Secret classification authority. Such delegation may only be made to officials who are determined to have a demonstrable and continuing need to exercise such authority.

(ii) *Secret and Confidential.* Only the Secretary of Defense, the Secretaries of the Military Departments, the senior official designated by each under §5.3(a) of E.O. 12356, and officials with original Top Secret classification authority, may delegate original Secret and Confidential classification authority to officials whom they determine respectively to have a demonstrable and continuing need to exercise such authority.

(iii) Each delegation of original classification authority shall be in writing and shall specify the title of the position held by the recipient.

(3) *Requests for Classification Authority*. (i) A request for the delegation of original classification authority shall be made only when there is a demonstrable and continuing need to exercise such authority and the following conditions exist:

(A) The normal course of operations or missions of the organization results in the origination of information warranting classification;

(B) There is a substantial degree of local autonomy in operations or missions as distinguished from dependence upon a higher level of command or supervision for relatively detailed guidance;

(C) There is adequate knowledge by the originating level to make sound classification determinations as distinguished from having to seek such knowledge from a higher level of command or supervision; and

(D) There is a valid reason why already designated classification authorities in the originator's chain of command or supervision have not issued or cannot issue classification guidance to meet the originator's normal needs.

(ii) Each request for a delegation of original classification authority shall:

(A) Identify the title of the position held by the nominee and the nominee's organization;

(B) Contain a description of the circumstances, consistent with paragraph (a)(3)(i) of this section, that justify the delegation of such authority; and

(C) Be submitted through established channels to the Secretary of Defense, the Secretary of the Military Department concerned, the senior official designated by each under §5.3(a) of E.O. 12356, or the appropriate Top Secret classification authority.

(4) *Training Requirements for Original Classification Authorities*. Heads of DoD Component shall establish procedures to ensure that all original classification authorities in their Component, to include themselves, are indoctrinated in the fundamentals of security classification, limitations on their authority to classify information, and their responsibilities as such. This indoctrination shall be a prerequisite to the exercise of such authority and shall be a matter of record that is subject to audit. Heads of DoD Components shall ensure this indoctrination is given to all present original classification authorities within 12 months of the effective date of this part.

(b) *Derivative Classification Responsibility*. Derivative application of classification markings is a responsibility of those who incorporate, paraphrase, restate, or generate in new form, information that is already classified, or those who apply markings in accordance with guidance from an original classification authority. Persons who apply derivative classifications should take care to determine whether their paraphrasing, restating, or summarizing of classified information has removed all or part of the basis for classification. Persons who apply such derivative classification markings shall:

(1) Respect original classification decisions;

(2) Verify the information's current level of classification as far as practicable before applying the markings; and

(3) Carry forward to any newly created documents the assigned dates or events for declassification and any additional authorized markings.

(c) *Record and Report Requirements.* (1) Records of designations of original classification authority shall be maintained as follows:

(i) *Top Secret Authorities.* A current listing by title and organization of officials designated to exercise original Top Secret classification authority shall be maintained by:

(A) The Office of the Deputy Under Secretary of Defense (Policy) (ODUSD(P)) for the Office of the Secretary of Defense; the Organization of the Joint Chiefs of Staff; the headquarters of each Unified Command and the headquarters of subordinate Joint Commands; and the Defense Agencies.

(B) The Offices of the Secretaries of the Military Departments for the officials of their respective departments, including Specified Commands but excluding officials from their respective

departments wo are serving in headquarters elements of Unified Commands and headquarters of Joint Commands subordinate thereto.

(ii) *Secret and Confidential Authorities.* A current listing by title and organization of officials designated to exercise original Secret and Confidential classification authority shall be maintained by:

(A) The ODUSD(P) for the Office of the Secretary of Defense.

(B) The offices of the Secretaries of the Military Departments for the officials of their respective departments, including Specified Commands but excluding officials from their respective departments who are serving in headquarters elements of Unified Commands and headquarters elements of Joint Commands subordinate thereto.

(C) The Director, Joint Staff, for the OJCS.

(D) The Commanders-in-Chief of the Unified Commands, for their respective headquarters and the headquarters of subordinate Joint Commands.

(E) The Directors of the Defense Agencies, for their respective agencies.

(iii) If the listing of titles of positions and organizations prescribed in paragraphs (c)(1) (i) and (ii) of this section discloses intelligence or other information that either qualifies for security classification protection or otherwise qualifies to be withheld from public release under statute, some other means may be recommended by the DoD Component by which original classification authorities can be readily identified. Such recommendations shall be submitted to ODUSD(P) for approval.

(iv) The listings prescribed in paragraphs (c)(1) (i) and (ii) of this section shall be reviewed at least annually by the senior official designated in or pursuant to § 159a.92(a)(1), § 159a.93 (a) or (b) or designee to ensure that officials so listed have demonstrated a continuing need to exercise original classification authority.

(2) The DoD Components that maintain listings of designated original classification authorities shall, upon request, submit copies of such listings to ODUSD(P).

(d) *Declassification and Downgrading Authority.* (1) Authority to declassify and downgrade information classified under provisions of this part shall be exercised as follows:

(i) By the Secretary of Defense and the Secretaries of the Military Departments, with respect to all information over which their respective Departments exercise final classification jurisdiction;

(ii) By the official who authorized the original classification, if that official is still serving in the same position, by a successor, or by a supervisory official of either; and

(iii) By other officials designated for the purpose in accordance with paragraph (d)(2) of this section.

(2) The Secretary of Defense, the Secretaries of the Military Departments, the Chairman of the Joint Chiefs of Staff, the Directors of the Defense Agencies, or their senior officials designated under § 159a.93 (b) or (c) may designate additional officials at the lowest practicable echelons of command and supervision to exercise declassification and downgrading authority over classified information in their functional areas of interest. Records of officials so designated shall be maintained in the same manner as prescribed in § 159a.12(c)(1)(i) for records of designations of original classification authority.

Subpart C—Classification

§ 159a.14 Classification responsibilities.

(a) *Accountability of Classifiers.* (1) Classifiers are accountable for the propriety of the classifications they assign, whether by exercise of original classification authority or by derivative classification.

(2) An official who classifies a document or other material and is identified thereon as the classifier is and continues to be an accountable classifier even though the document or material is approved or signed at a higher level in the same organization.

(b) *Classification Approval.* (1) When an official signs or approves a document or other material already marked to reflect a particular level of classification, he or she shall review the information contained therein to determine if the classification markings are

appropriate. If, in his or her judgment, the classification markings are not supportable, he or she shall, at that time, cause such markings to be removed or changed as appropriate to reflect accurately the classification of the information involved.

(2) A higher level official through or to whom a document or other material passes for signature or approval becomes jointly responsible with the accountable classifier for the classification assigned. Such official has discretion to decide whether a subordinate who has classification authority shall be identified as the accountable classifier when he or she has exercised that authority.

(c) *Classification Planning.* (1) Advance classification planning is an essential part of the development of any plan, operation, program, research and development project, or procurement action that involves classified information. Classification must be considered from the outset to assure adequate protection for the information and for the activity itself, and to eliminate impediments to the execution or implementation of the plan, operations order, program, project or procurement action.

(2) The official charged with developing any plan, program or project in which classification is a factor, shall include under an identifiable title or heading, classification guidance covering the information involved. The guidance shall conform to the requirements contained in §159a.17.

(d) *Challenges to Classification.* If holders of classified information have substantial reason to believe that the information is classified improperly or unnecessarily, they shall communicate that belief to their security manager or the classifier of the information to bring about any necessary correction.

(1) Each DoD Component shall establish procedures whereby holders of classified information may challenge the decision of the classifier.

(2) Challenges to classification made under this subsection shall include sufficient description of the information being challenged to permit identification of the information and its classifier with reasonable effort. Challenges to classification shall also include the reason or reasons why the challenger believes that the information is classified improperly or unnecessarily.

(3) Challenges received under this subsection shall be acted upon within 30 days of receipt. The challenger shall be notified of any changes made as a result of the challenge or the reasons why no change is made.

(4) Pending final determination of a challenge to classification, the information or document in question shall be safeguarded as required for the level of classification initially assigned.

(5) The fact that an employee or military member of the Department of Defense has issued a challenge to classification shall not in any way result in or serve as a basis for adverse personnel action.

(6) The provisions of this paragraph do not apply to or affect declassification review actions undertaken under the mandatory review requirements of §159a.26 of this part or under the provisions of 32 CFR part 285.

§159a.15 Classification principles, criteria, and considerations.

(a) *Reasoned Judgment.* Reasoned judgment shall be exercised in making classification decisions. A positive basis must exist for classification. Both advantages and disadvantages of classification must be weighed. If, after consideration of the provisions of this section, there is reasonable doubt, the provisions of §159a.10(a)(2) apply.

(b) *Identification of Specific Information.* Before a classification determination is made, each item of information that may require protection shall be identified. This requires identification of that specific information that comprises the basis for a particular national advantage or advantages that, if the information were compromised, would or could be damaged, minimized, or lost, thereby adversely affecting national security.

(c) *Specific Classifying Criteria.* A determination to classify shall be made only by an original classification authority when, *first*, the information is within paragraphs (c) (1) through (10) of this section; and *second*, the unauthorized disclosure of the information, either by itself or in the context of other

information, reasonably could be expected to cause damage to the national security. The determination involved in the first step is separate and distinct from that in the second. Except as provided in paragraph (d) of this section, the fact that the information falls under one or more of the criteria shall not mean that the information *automatically* meets the damage criteria. Information shall be considered for classification if it concerns:

(1) Military plans, weapons, or operations;

(2) Vulnerabilities or capabilities of systems, installations, projects, or plans relating to the national security;

(3) Foreign government information;

(4) Intelligence activities including special activities, or intelligence sources or methods;

(5) Foreign relations or foreign activities of the United States;

(6) Scientific, technological, or economic matters relating to the national security;

(7) U.S. Government programs for safeguarding nuclear materials or facilities;

(8) Cryptology;

(9) A confidential source; or

(10) Other categories of information that are related to national security and that require protection against unauthorized disclosure as determined by the Secretary of Defense or Secretaries of the Military Departments. Recommendations concerning the need to designate additional categories of information that may be considered for classification shall be forwarded through channels to the appropriate Secretary for determination. Each such determination shall be reported promptly to the Director of Security Plans and Programs, ODUSD(P), for promulgation in an Appendix to this part and reporting to the Director, ISOO.

(d) *Presumption of Damage.* Unauthorized disclosure of foreign government information, the identity of a confidential foreign source, or intelligence sources or methods is presumed to cause damage to the national security.

(e) *Limitations on Classification.* (1) classification may not be used to conceal violations of law, inefficiency, or administrative error, to prevent embarrassment to a person, organization or agency, or to restrain competition.

(2) Basic scientific research information not clearly related to national security may not be classified.

(3) A product of nongovernment research and development that does not incorporate or reveal classified information to which the producer or developer was given prior access may not be classified until and unless the government acquires a proprietary interest in the product. This prohibition does not affect the provisions of the Patent Secrecy Act of 1952.

(4) References to classified documents that do not reveal classified information may not be classified or used as a basis for classification.

(5) Classification may not be used to limit dissemination of information that is not classifiable under the provisions of E.O. 12356 or this part or to prevent or delay public release of such information.

(6) Information may be classified or reclassified after receiving a request for it under the Freedom of Information Act, the Privacy Act, or the mandatory review provisions of this part (§ 159a.26) if such classification is consistent with this part and is accomplished personally and on a document-by-document basis, except as provided in paragraph (e)(7) of this section, by the Secretary or Deputy Secretary of Defense, by the Secretaries or Under Secretaries of the Military Departments, by the senior official designated by each Secretary under § 5.3(a) of E.O. 12356, or by an official with original Top Secret classification authority.

(7) The Secretary of Defense and the Secretaries of the Military Departments may reclassify information previously declassified and disclosed, and they may classify unclassified information that has been disclosed, if they determine in writing that the information requires protection in the interest of national security and the information may reasonably be recovered. Any such reclassification or classification shall be reported to the DUSD(P) for subsequent reporting to the Director, ISOO.

(f) *Classifying Scientific Research Data.* Ordinarily, except for information that meets the definition of Restricted

Data, basic scientific research or its results shall not be classified. However, classification would be appropriate if the information concerns an unusually significant scientific breakthrough and there is sound reason to believe that it is not known or within the state-of-the-art of other nations, and it supplies the United States with an advantage directly related to national security.

(g) *Classifying Documents.* Each document and portion thereof shall be classified on the basis of the information it contains or reveals. The fact that a document makes reference to a classified document is not a basis for classification unless the reference citation, standing alone, reveals classified information. The overall classification of a document or group of physically-connected documents shall be at least as high as that of the most highly classified component. The subject or title of a classified document normally should be unclassified. When the information revealed by a subject or title warrants classification, an unclassified short title should be added for reference purposes.

(h) *Classifying Material Other Than Documents.* (1) Items of equipment or other physical objects shall be classified only when classified information may be derived from them by visual observation of their internal or external appearance or structure, or by their operation, test, application, or use. The overall classification assigned to end items of equipment or objects shall be at least as high as the highest classification of any of its integrated parts.

(2) If mere knowledge of the existence of the item of equipment or object would compromise or nullify its national security advantage, its existence would warrant classification.

(i) *State of the Art and Intelligence.* Classification requires consideration of the information available from intelligence sources concerning the extent to which the same or similar information is known or is available to others. It is also important to consider whether it is known, publicly or internationally, that the United States has the information or even is interested in the subject matter. The state-of-the-art in other nations may often be a vital consideration.

(j) *Effect of Open Publication.* Classified information shall not be declassified automatically as a result of any unofficial publication or inadvertent or unauthorized disclosure in the United States or abroad of identical or similar information. Appearance in the public domain of information currently classified or being considered for classification does not preclude initial or continued classification. However, such disclosures require immediate determination of the degree of damage to the national security and reevaluation of the information to determine whether the publication has so compromised the information that downgrading or declassification is warranted. Similar consideration must be given to related items of information in all programs, projects, or items incorporating or pertaining to the compromised items of information. Holders should continue classification until advised to the contrary by a competent government authority.

(k) *Reevaluation of Classification Because of Compromise.* Classified information, and information related thereto, that has been lost or possibly compromised, shall be reevaluated and acted upon as follows:

(1) The original classifying authority, upon learning that a loss or possible compromise of specific classified information has occurred, shall prepare a written damage assessment and;

(i) Reevaluate the information involved and determine whether (A) Its classification should be continued without change; (B) The specific information, or parts therof, should be modified to minimize or nullify the effects of the reported compromise and the classification retained; (C) Declassification, downgrading, or upgrading is warranted; and (D) Counter-measures are appropriate and feasible to negate or minimize the effect of the compromise.

(ii) Give prompt notice to all holders of such information when the determination is within categories (A), (C), or (D) of paragraph (k)(1)(i) of this section.

(2) Upon learning that a compromise or probable compromise has occurred,

any official having original classification jurisdiction over related information shall reevaluate the related information and determine whether one of the courses of action enumerated in paragraph (k)(1)(i) of this section should be taken or, instead, whether upgrading of the related information is warranted. When such a determination is within categories (B), (C), or (D) of paragraph (k)(1)(i) of this section, that upgrading of the related items is warranted, prompt notice of the determination shall be given to all holders of the related information.

(l) *Compilation of Information*. Certain information that would otherwise be unclassified may require classification when combined or associated with other unclassified information. However, a compilation of unclassified items of information should normally not be classified. In unusual circumstances, classification may be required if the combination of unclassified items of information provides an added factor that warrants classification under paragraph (c) of this section. Classification on this basis shall be fully supported by a written explanation that will be provided with the material so classified.

(m) *Extracts of Information*. Information extracted from a classified source shall be derivatively classified or not classified in accordance with the classification markings shown in the source. The overall and internal markings of the source should supply adequate classification guidance. If internal markings or classification guidance are not found in the source, and no reference is made to an applicable and available classification guide, the extracted information shall be classified according either to the overall marking of the source, or guidance obtained from the classifier of the source material.

§ 159a.16 Duration of original classification.

(a) *General*. When a determination is made by an official with authority to classify originally information as Top Secret, Secret, or Confidential, such official must also determine how long the classification shall remain in effect.

(b) *Duration of Classification*. (1) Information shall be classified as long as required by national security considerations.

(2) When it can be determined, a specific date or event for declassification shall be set by the original classification authority at the time the information is classified originally. Such dates or events shall be consistent with national security. Any event specified for declassification shall be an event certain to occur.

(3) Original classification authorities may not be able to predetermine a date or event for automatic declassification in which case they shall provide for the indefinite duration of classification.

(4) Information classified under predecessor orders and marked for declassification review shall remain classified until reviewed for declassification under the provisions of this part.

(c) *Subsequent Extension of Duration of Classification*. The duration of classification specified at the time of original classification may be extended only by officials with requisite original classification authority and only if all known holders of the information can be notified of such action before the date or event previously set for declassification. Any decision to continue classification of information designated for automatic declassification under E.O. 12065 or predecessor orders, other than on a document-by-document basis, shall be reported to the DUSD(P) who shall, in turn, report to the Director, ISOO.

§ 159a.17 Classification guides.

(a) *General*. (1) A classification guide shall be issued for each classified system, program, plan, or project as soon as practicable before the initial funding or implementation of the system, program, plan or project. Successive operating echelons shall prescribe more detailed supplemental guides that are considered essential to assure accurate and consistent classification. In preparing classification guides, originators shall review DoD 5200.1–H[5].

(2) Classification guides shall:

(i) Identify the information elements to be protected, using categorization to

[5] See footnote 2 to § 159a.3.

the extent necessary to ensure that the information involved can be identified readily and uniformly;

(ii) State which the classification designations (that is, Top Secret, Secret, or Confidential) applies to each element or category of information;

(iii) State declassification instructions for each element or category of information in terms of a period of time, the occurrence of an event, or a notation that the information shall not be declassified automatically without approval of the originating agency; and

(iv) State any special public release procedures and foreign disclosure considerations.

(3) Each classification guide shall be approved personally and in writing by an official who:

(i) Has program or supervisory responsibility over the information or is the senior agency official designated by the Secretary of Defense or Secretaries of the Military Departments in accordance with §5.3(a) of E.O. 12356; and

(ii) Is authorized to classify information originally at the highest level of classification prescribed in the guide.

(b) *Multiservice Interest.* For each classified system, program, project, plan, or item involving more than one DoD Component, a classification guide shall be issued by: (1) The element in the Office of the Secretary of Defense that assumes or is expressly designated to exercise overall cognizance over it; or (2) The DoD Component that is expressly designated to serve as the executive or administrative agent for the particular effort. When there is doubt which Component has cognizance of the information involved, the matter shall be referred to the DUSD(P) for resolution.

(c) *Research, Development, Test, and Evaluation.* A program security classification guide shall be developed for each system and equipment development program that involves research, development, test, and evaluation (RDT&E) of classified technical information. For each such program covered by an approved Decision Coordinating Paper (DCP) or Program Objective Memorandum (POM), initial basic classification guidance applicable to technical characteristics of the system or equipment shall be developed and submitted with the proposed DCP or POM to the Director, Defense Research and Engineering for approval. A detailed classification guide shall be developed and issued as near in time as possible to the approval of the DCP or POM.

(d) *Project Phases.* Whenever possible, classification guides shall cover specifically each phase of transition, that is, RDT&E, procurement, production, service use, and obsolescence, with changes in assigned classifications to reflect the changing sensitivity of the information involved.

(e) *Review of Classification Guides.* (1) Classification guides shall be reviewed by the originator for currency and accuracy not less than once every 2 years. Changes shall be issued promptly. If no changes are made, the originator shall so annotate the record copy and show the date of the review.

(2) Classification guides issued before August 1, 1982, that are in current use must be updated to meet the requirements of paragraph (a)(2) of this section. Such updating shall be accomplished by the next biennial review. Converting previous declassification determinations directed by classification guides shall be accomplished in accordance with the following:

(i) Automatic declassification dates or events remain in force unless changed by competent authority in accordance with §159a.16(c).

(ii) Dates for declassification review shall be changed to automatic declassification dates or provide for the indefinite duration of classification.

(f) *Distribution of Classification Guides.* (1) A copy of each approved classification guide and changes thereto other than those covering SCI or a Special Access Program and which discloses information that require special access, shall be sent to the Director of Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs), and to the Director of Security Plans and Programs, ODUSD(P). A copy of each approved classification guide covering SCI shall be submitted to and maintained by the Senior Intelligence Officer who has security cognizance over the issuing activity.

(2) Two copies of each approved classification guide and its changes shall be sent by the originator to the Administrator, Defense Technical Information Center (DTIC), Defense Logistic Agency, unless such guide is classified Top Secret, or covers SCI, or is determined by the approval authority of the guide to be too sensitive for automatic secondary distribution to DoD Components, such as a Special Access Program guide revealing the nature of the Program. Each classification guide forwarded to DTIC must bear distribution statement B, C, D, E, F, or X from DoD Directive 5230.24[6] on its front cover or first page if there is no cover.

(g) *Index of Security Classification Guides.* (1) All security classification guides, except as provided in paragraph (g)(2) of this section, issued under this part shall be listed in DoD 5200.1–I[7], on the basis of information provided on DD Form 2024, ''DoD Security Classification Guide Data Elements.'' The originator of each guide shall execute DD Form 2024 when the guide is approved, changed, revised, reissued, or canceled, and when its biennial review is accomplished. The original copy of each executed DD Form 2024 shall be forwarded to the Director of Security Plans and Programs, ODUSD(P) who will maintain the Index. Report Control Symbol DD–POL (B&AR)1418 applies to this information collection system.

(2) Any classification guide that because of classification considerations is not listed in accordance with paragraph (g)(1) of this section, shall be reported by the originator to the Director of Security Plans and Programs, ODUSD(P). The report shall include the title of the guide, its date, the classification of the guide, and identification of the originating activity. A separate classified list of such guides will be maintained. Report Control Symbol DD–POL(B&AR)1418 applies to this information collection system.

§ 159a.18 Resolution of conflicts.

(a) *General.* When two or more offices, headquarters, or activities disagree concerning a classification, declassification, or regrading action, the disagreement must be resolved promptly.

(b) *Procedures.* If agreement cannot be reached by informal consultation, the matter shall be referred for decision to the lowest superior common to the disagreeing parties. If agreement cannot be reached at the major command (or equivalent) level, the matter shall be referred for decision to the headquarters office having overall classification management responsibilities for the Component. That office shall also be advised of any disagreement at any echelon if prompt resolution is not likely to occur.

(c) *Final Decision.* Disagreements between DoD Component headquarters, if not resolved promptly, shall be referred for final resolution to the ODUSD(P).

(d) *Timing.* Action under this section at each level of consideration shall be completed within 30 days. Failure to reach a decision within 30 days shall be cause for referral to the next level for consideration.

§ 159a.19 Obtaining classification evaluations.

Procedures. If a person not authorized to classify originates or develops information that he or she believes should be safeguarded, he or she shall:

(a) Safeguard the information in the manner prescribed for the intended classification.

(b) Mark the information (or cover sheet) with the intended classification designation prescribed in § 159a.11;

(c) Transmit the information under appropriate safeguards to an appropriate classification authority for evaluation. The transmittal shall state that the information is tentatively marked to protect it in transit. If such authority is not readily identifiable, the information should be forwarded to a headquarters activity of a DoD Component, to the headquarters office having overall classification management responsibilities for a DoD Component, or to the DUSD(P). A determination whether to classify the information shall be made within 30 days of receipt;

(d) Upon decision by the classifying authority, the tentative marking shall be removed. If a classification is assigned, appropriate markings shall be applied; but

[6] See footnote 1 to § 159a.3.

[7] Controlled distribution.

(e) In an emergency requiring immediate communication of the information, after taking the action prescribed by paragraphs (a) and (b) of this section transmit the information and then proceed in accordance with paragraph (c) of this section.

§ 159a.20 Information developed by private sources.

(a) *General.* There are some circumstances in which information not meeting the definition in § 159a.9(f) may warrant protection in the interest of national security.

(b) *Patent Secrecy Act.* The Patent Secrecy Act of 1952 provides that the Secretary of Defense, among others, may determine that disclosure of an invention by granting of a patent would be detrimental to national security. See DoD Directive 5535.2[8]. A patent application on which a secrecy order has been imposed shall be handled as follows within the Department of Defense:

(1) If the patent application contains information that warrants classification, it shall be assigned a classification and be marked and safeguarded accordingly.

(2) If the patent application does not contain information that warrants classification, the following procedures shall be followed:

(i) A cover sheet (or cover letter for transmittal) shall be placed on the application with substantially the following language:

> The attached material contains information on which secrecy orders have been issued by the U.S. Patent Office after determination that disclosure would be detrimental to national security (Patent Secrecy Act of 1952, 35 U.S.C. 181–188). Its transmission or revelation in any manner to an unauthorized person is prohibited by law. Handle as though classified CONFIDENTIAL (or such other classification as would have been assigned had the patent application been within the definition provided in § 159a.9(f)).

(ii) The information shall be withheld from public release; its dissemination within the Department of Defense shall be controlled; the applicant shall be instructed not to disclose it to any unauthorized person; and the patent application (or other document incorporating the protected information) shall be safeguarded in the manner prescribed for equivalent classified material.

(3) If filing of a patent application with a foreign government is approved under provisions of the Patent Secrecy Act of 1952 and agreements on interchange of patent information for defense purposes, the copies of the patent application prepared for foreign registration (but only those copies) shall be marked at the bottom of each page as follows:

> Withheld under the Patent Secrecy Act of 1952 (35 U.S.C. 181–188). Handle as CONFIDENTIAL (or such other level as has been determined).

(c) *Independent Research and Development.* (1) Information in a document or material that is a product of government-sponsored independent research and development conducted without access to classified information may not be classified unless the government first acquires a proprietary interest in such product.

(2) If no prior access was given but the person or company conducting the independent research or development believes that protection may be warranted in the interest of national security, the person or company should safeguard the information in accordance with § 159a.19 and submit it to an appropriate DoD element for evaluation. The DoD element receiving such a request for evaluation shall make or obtain a determination whether a classification would be assigned if it were government information. If the determination is negative, the originator shall be advised that the information is unclassified. If the determination is affirmative, the DoD element shall make or obtain a determination whether a proprietary interest in the research and development will be acquired. If so, the information shall be assigned proper classification. If not, the originator shall be informed that there is no basis for classification and the tentative classification shall be canceled.

(d) *Other Private Information.* The procedure specified in § 159a.19 shall apply in any case not specified in paragraph

[8] See footnote 1 to § 159a.3.

(c) of this section, such as an unsolicited contract bid, in which private information is submitted to a DoD element for a determination of classification.

§ 159a.21 Regrading.

(a) *Raising to a Higher Level of Classification.* The upgrading of classified information to a higher level than previously determined by officials with appropriate classification authority and jurisdiction over the subject matter is permitted only when all known holders of the information:

(1) Can be notified promptly of such action, and

(2) Are authorized access to the higher level of classification, or the information can be retrieved from those not authorized access to information at the contemplated higher level of classification.

(b) *Classification of Information Previously Determined to be Unclassified.* Unclassified information, once communicated as such, may be classified only when the classifying authority:

(1) Makes the determination required for upgrading in paragraph (a) of this section;

(2) Determines that control of the information has not been lost by such communication and can still be prevented from being lost; and

(3) In the case of information released to secondary distribution centers, such as the DTIC, determines that no secondary distribution has been made and can still be prevented (see also § 159a.15(e) (6) and (7)).

(c) *Notification.* All known holders of information that has been upgraded shall be notified promptly of the upgrading action.

(d) *Downgrading.* When it will serve a useful purpose, original classification authorities may, at the time of original classification, specify that downgrading of the assigned classification will occur on a specified date or upon the occurrence of a stated event.

§ 159a.22 Industrial operations.

(a) *Classification in Industrial Operations.* Classification of information in private industrial operations shall be based only on guidance furnished by the government. Industrial management may not make original classification determinations and shall implement the classification decisions of the U.S. Government contracting authority.

(b) *Contract Security Classification Specification.* DD Form 254, ''Contract Security Classification Specification,'' shall be used to convey contractual security classification guidance to industrial management. DD Forms 254 shall be changed by the originator to reflect changes in classification guidance and reviewed for currency and accuracy not less than once every 2 years. Changes shall conform with this part and DoD 5220.22–R and DoD 5220.22–M and shall be provided to all holders of the DD Form 254 as soon as possible. When no changes are made as a result of the biennial review, the originator shall so notify all holders of the DD Form 254 in writing.

Subpart D—Declassification and Downgrading

§ 159a.24 General provisions.

(a) *Policy.* Information classified under E.O. 12356 and prior orders shall be declassified or downgraded as soon as national security considerations permit. Decisions concerning declassification shall be based on the loss of sensitivity of the information with the passage of time or on the occurrence of an event that permits declassification. Information that continues to meet the classification requirements of § 159a.15(c) despite the passage of time will continue to be protected in accordance with this part.

(b) *Responsibility of Officials.* Officials authorized under § 159a.12(c) to declassify or downgrade information that is under the final classification jurisdiction of the Department of Defense shall take such action in accordance with this subpart.

(c) *Declassification Coordination.* DoD Component declassification review of classified information shall be coordinated with any other DoD or non-DoD office, Component, or agency that has a direct interest in the subject matter.

(d) *Declassification by the Director of the ISOO.* If the Director of the ISOO

determines that information is classified in violation of E.O. 12356, the Director may require the activity that originally classified the information to declassify it. Any such decision by the Director may be appealed through the Director of Security Plans and Programs, ODUSD(P), to the National Security Council (NSC). The information shall remain classified pending a prompt decision on the appeal.

§ 159a.25 Systematic review.

(a) *Assistance to the Archivist of the United States.* The Secretary of Defense and the Secretaries of the Military Departments shall designate experienced personnel to assist the Archivist of the United States in the systematic review of classified information. Such personnel shall:

(1) Provide guidance and assistance to National Archives and Records Administration (NARA) employees in identifying and separating documents and specific categories of information within documents that are deemed to require continued classification; and

(2) Refer doubtful cases to the DoD Component having classification jurisdiction over the information or material for resolution.

(b) *Systematic Review Guidelines.* The Director of Security Plans and Programs, ODUSD(P), in coordination with DoD Components, shall review, evaluate, and recommend revisions of DoD Directive 5200.30[9] at least every 5 years.

(c) *Systematic Review Procedures.* (1) Except as noted in this subsection, classified information transferred to the NARA that is permanently valuable will be reviewed systematically for declassification by the Archivist of the United States with the assistance of the DoD personnel designated for that purpose under paragraph (a) of this section as it becomes 30 years old. Information concerning intelligence (including special activities), sources, or methods created after 1945, and information concerning cryptology created after 1945, accessioned into the NARA will be reviewed systematically as it becomes 50 years old. Such information shall be downgraded or declassified by the Archivist of the United States under E.O. 12356, the directives of the ISOO, and DoD Directive 5200.30.

(2) All DoD classified information that is permanently valuable and in the possession or control of DoD Components, including that held in Federal Records Centers or other storage areas, may be reviewed systematically for declassification by the DoD Component exercising control of such information. Systematic declassification review conducted by DoD Components and personnel designated under paragraph (a) of this section shall proceed as follows:

(i) Information over which the Department of Defense exercises exclusive or final original classification authority and that under DoD Directive 5200.30, the responsible reviewer determines is to be declassified, shall be marked accordingly.

(ii) Information over which the Department of Defense exercises exclusive or final original classification authority that, after review, is determined to warrant continued protection shall remain classified as long as required by national security considerations.

(3) Classified information over which the Department of Defense does not exercise exclusive or final original classification authority encountered during DoD systematic review may not be declassified unless specifically authorized by the agency having classification jurisdiction over it.

(d) *Systematic Review of Classified Cryptologic Information.* Notwithstanding any other provision of this part, systematic review and declassification of classified cryptologic information shall be conducted in accordance with special procedures developed in consultation with affected agencies by the Director, National Security Agency/Chief, Central Security Service, and approved by the Secretary of Defense under E.O. 12356 and DoD Directive 5200.30.

(e) *Systematic Review of Intelligence Information.* Systematic review for declassification of classified information pertaining to intelligence activities (including special activities), or intelligence sources or methods shall be in accordance with special procedures to

[9] See footnote 1 to § 159a.3.

be established by the Director of Central Intelligence after consultation with affected agencies.

§ 159a.26 Mandatory declassification review.

(a) *Information Covered.* Upon request by a U.S. citizen or permanent resident alien, a Federal agency, or a State or local government to declassify and release such information, any classified information (except as provided in paragraph (b) of this section) shall be subject to review by the originating or responsible DoD Component for declassification in accordance with this section.

(b) *Presidential Information.* Information originated by a President, the White House staff, committees, commissions, or boards appointed by the President, or others specifically providing advice and counsel to a President or acting on behalf of a President is exempt from the provisions of this section.

(c) *Cryptologic Information.* Requests for the declassification review of cryptologic information shall be processed in accordance with the provisions of DoD Directive 5200.30.

(d) *Submission of Requests for Mandatory Declassification Review.* Requests for mandatory review of DoD classified information shall be submitted as follows:

(1) Requests shall be in writing and reasonably describe the information sought with sufficient particularity to enable the Component to identify documents containing that information, and be reasonable in scope; for example, the request does not involve such a large number or variety of documents as to leave uncertain the identity of the particular information sought.

(2) Requests shall be submitted to the Office of the Assistant Secretary of Defense (Public Affairs) (ASD(PA)) (entry point for OSD records), the Military Department, or other Component most concerned with the subject matter that is designated under 32 CFR part 285 to receive requests for records under the Freedom of Information Act. These offices are identified in appropriate parts of title 32 of the Code of Federal Regulations for each DoD Component.

(e) *Requirements for Processing.* Unless otherwise directed by the ASD(PA), requests for mandatory review shall be processed as follows:

(1) The designated office shall acknowledge receipt of the request. When a request does not satisfy the conditions of paragraph (d)(1) of this section, the requester shall be notified that unless additional information is provided or the scope of the request narrowed, no further action will be undertaken.

(2) DoD Component action upon the initial request shall be completed within 60 days (45 working days). If no determination has been made within 60 days (45 working days) of receipt of the request, the requester shall be notified of his right to appeal and of the procedures for making such an appeal.

(3) The designated office shall determine whether, under the declassification provisions of this part, the requested information may be declassified, and, if so, make such information available to the requester, unless withholding is otherwise warranted under applicable law. If the information may not be released in whole or in part, the requester shall be given a brief statement as to the reasons for denial, notice of the right to appeal the determination within 60 days (45 working days) to a designated appellate authority (including name, title, and address of such authority), and the procedures for such an appeal.

(4) When a request is received for information classified by another DoD Component or an agency outside the Department of Defense, the designated office shall:

(i) Forward the request to such DoD Component or outside agency for review together with a copy of the document containing the information requested, when practicable and when appropriate, with its recommendation to withhold any of the information;

(ii) Notify the requester of the referral unless the DoD Component or outside agency to which the request is referred objects to such notice on grounds that its association with the information requires protection; and

(iii) Request, when appropriate, that the DoD Component or outside agency notify the referring office of its determination.

(5) If the request requires the rendering of services for which fees may be charged under title 5 of the Independent Offices Appropriation Act in accordance with DoD Instruction 7230.7[10] the DoD Component may calculate the anticipated amount of fees to be charged and ascertain the requester's willingness to pay the allowable charges as a precondition to taking further action upon the request.

(6) A requester may appeal to the head of a DoD Component or designee whenever that DoD Component has not acted on an initial request within 60 days or the requester has been notified that requested information may not be released in whole or in part. Within 30 days after receipt, an appellate authority shall determine whether continued classification of the requested information is required in whole or in part, notify the requester of its determination, and make available to the requester any information determined to be releasable. If continued classification is required under this part, the requester shall be notified of the reasons therefor. If so requested, an appellate authority shall communicate its determination to any referring DoD Component or outside agency.

(7) The ASD(PA) shall act as appellate authority for all appeals regarding OSD, OJCS, and Unified Command records.

(f) *Foreign Government Information.* Requests for mandatory review for the declassification of foreign government information shall be processed and acted upon under the provisions of this section subject to §159a.76(c).

(g) *Prohibition.* No DoD Component in possession of a document shall in response to a request under the Freedom of Information Act or this section refuse to confirm the existence or nonexistence of the document, unless the fact of its existence or nonexistence would itself be classifiable under this part.

(h) *Restricted Data and Formerly Restricted Data.* Any proposed action on a request, including requests from Presidential libraries, for DoD classified documents that are marked ''Restricted Data'' or ''Formerly Restricted Data'' must be coordinated with the Department of Energy.

[10] See footnote 1 to §159a.3

§159a.27 Declassification of transferred documents or material.

(a) *Material Officially Transferred.* In the case of classified information or material transferred under statute, E.O., or directive from one department or agency or DoD Component to another in conjunction with a transfer of functions, as distinguished from transfers merely for purposes of storage, the receiving department, agency, or DoD Component shall be deemed to be the original classifying authority over such material for purposes of downgrading and declassification.

(b) *Material Not Officially Transferred.* When a DoD Component has in its possession classified information or material originated in an agency outside the Department of Defense that has ceased to exist and such information or material has not been transferred to another department or agency within the meaning of paragraph (a) of this section, or when it is impossible to identify the originating agency, the DoD Component shall be deemed to be the originating agency for the purpose of declassifying or downgrading such information or material. If it appears probable that another department, agency, or DoD Component may have a substantial interest in the classification of such information, the DoD Component deemed to be the originating agency shall notify such other department, agency, or DoD Component of the nature of the information or material and any intention to downgrade or declassify it. Until 60 days after notification, the DoD Component shall not declassify or downgrade such information or material without consulting the other department, agency, or DoD Component. During this period, the other department, agency, or DoD Component may express objections to downgrading or declassifying such information or material.

(c) *Transfer for Storage or Retirement.* Whenever practicable, classified documents shall be reviewed for downgrading or declassification before they are forwarded to a Records Center for storage or to the NARA for permanent

preservation. Any downgrading or declassification determination shall be indicated on each document by markings as required by subpart E of this part.

§ 159a.28 Downgrading.

(a) *Automatic Downgrading.* Classified information marked for automatic downgrading in accordance with this or prior regulations or E.Os. is downgraded accordingly without notification to holders.

(b) *Downgrading Upon Reconsideration.* Classified information not marked for automatic downgrading may be assigned a lower classification designation by the originator or by an official authorized to declassify the same information. Prompt notice of such downgrading shall be provided to known holders of the information.

§ 159a.29 Miscellaneous.

(a) *Notification of Changes in Declassification.* When clasified material has been properly marked with specific dates or events for declassification, it is not necessary to issue notices of declassification to any holders. However, when declassification action is taken earlier than originally scheduled, or the duration of classification is extended, the authority making such changes shall ensure prompt notification of all holders to whom the information was originally transmitted. The notification shall specify the marking action to be taken, the authority therefor, and the effective date. Upon receipt of notification, recipients shall effect the proper changes and shall notify holders to whom they have transmitted the classified information. See § 159a.34 (a) and (e) for markings and the use of posted notices.

(b) *Foreign Relations Series.* In order to permit the State Department editors of *Foriegn Relations of the United States* to meet their mandated goal of publishing twenty years after the event, DoD Components shall assist the editors in the Department of State by easing access to appropriate classified materials in their custody and by expediting declassification review of items from their files selected for possible publication.

(c) *Reproduction for Declassification Review.* The provisions of § 159a.55(f) shall not restrict the reproduction of documents for the purpose of facilitating declassification review under the provisions of this subpart or the Freedom of Information Act, as amended. After review for declassification, however, those reproduced documents that remain classified must be destroyed in accordance with subpart J of this part.

Subpart E—Marking

§ 159a.31 General provisions.

(a) *Designation.* Subject to the exceptions in paragraph (c) of this section, information determined to require classification protection under this part shall be so designated. Designation by means other than physical marking may be used but shall be followed by physical marking as soon as possible.

(b) *Purpose of Designation.* Designation by physical marking, notation, or other means serves to warn the holder about the classification of the information involved; to indicate the degree of protection against unauthorized disclosure that is required for that particular level of classification; and to facilitate downgrading and declassification actions.

(c) *Exceptions.* (1) No article that has appeared, in whole or in part, in newspapers, magazines or elsewhere in the public domain, or any copy thereof, that is being reviewed and evaluated to compare its content with classified information that is being safeguarded in the Department of Defense by security classification, may be marked with any security classification, control or other kind of restrictive marking. The results of the review and evaluation, if classified, shall be separate from the article in question.

(2) Classified documents and material shall be marked in accordance with paragraph (d) of this section unless the markings themselves would reveal a confidential source or relationship not otherwise evident in the document, material, or information.

(3) The marking requirements of paragraph (d) (1)(iv) and (2)(iv) of this section do not apply to documents or

other material that contain, in whole or in part, Restricted Data or Formerly Restricted Data information. Such documents or other material or portions thereof shall not be declassified without approval of the Department of Energy with respect to Restricted Data or Formerly Restricted Data information, and with respect to any other national security information contained therein, the approval of the originating agency.

(d) *Documents or Other Material in General.* (1) At the time of original classification, the following shall be shown on the face of all originally classified documents or clearly associated with other forms of classified information in a manner appropriate to the medium involved:

(i) The identity of the original classification authority by position title, unless he or she is the signer or approver of the document;

(ii) The agency and office of origin;

(iii) The overall classification of the document;

(iv) The date or event for automatic declassification or the notation ''Originating Agency's Determination Required'' or ''OADR''; and, if applicable,

(v) Any downgrading action to be taken and the date or event thereof.

(2) At the time of derivative classification, the following shall be shown on the face of all derivatively classified documents or clearly associated with other forms of classified information in a manner appropriate to the medium involved:

(i) The source of classification, that is, a source document or classification guide. If classification is derived from more than one source, the phrase ''Multiple Sources'' will be shown and the identification of each source will be maintained with the file or record copy of the document;

(ii) The agency and office of origin of the derivatively classified document;

(iii) The overall classification of the document;

(iv) The date or event for declassification or the notation ''Originating Agency's Determination Required'' or ''OADR,'' carried forward from the classification source. If the classification is derived from multiple sources, either the most remote date or event for declassification marked on the sources or if required by any source, the notation ''Originating Agency's Determination Required'' or ''OADR'' shall be shown; and, if applicable,

(v) Any downgrading action to be taken and the date or event thereof.

(3) In addition to the foregoing, classified documents shall be marked as prescribed in §159a.32, subpart L of this part, if the document contains foreign government information, and with any applicable special notation listed in §159a.35. Such notations shall be carried forward from source documents to derivatively classified documents when appropriate. Provides illustrated guidance on the application of classification and associated markings to documents prepared by the Department of Defense.

(4) Material other than paper documents shall show the required information on the material itself or if that is not practical, in related or accompanying documentation.

(e) *Identification of Classification Authority.* (1) Identification of a classification authority shall be shown on the ''Classified by'' line prescribed under §159a.34(c) and shall be sufficient, standing alone, to identify a particular official, source document or classification guide.

(i) If all information in a document or material is classified as an act of original classification, the classification authority who made the determination shall be identified on the ''Classified by'' line, unless the classifier is also the signer or approver of the document.

(ii) If the classification of all information in a document or material is derived from a single source (for example, a source document or classification guide), the ''Classified by'' line shall identify the source document or classification guide, including its date when necessary to insure positive identification.

(iii) If the classification of information contained in a document or material is derived from more than one original classification authority, or an original classification authority and another source, or from more than one source document, classification guide, or combination thereof, the ''Classified

by'' line shall be marked ''Multiple Sources'' and identification of all such authorities and sources shall be maintained with the file or record copy of the document.

(iv) If an official with requisite classification authority has been designated by the head of an activity to approve security classifications assigned to all information leaving the activity, the title of that designated official shall be shown on the ''Classified by'' line. The designated official shall maintain records adequate to support derivative classification actions.

(2) Guidance concerning the identification of the classification authority on electronically transmitted messages is contained in §159a.32(h).

(3) Guidance concerning the identification of the classification authority on DoD documents that contain only foreign or NATO classified information is contained in §159a.77(d).

(f) *Wholly Unclassified Material.* Normally, unclassified material shall not be marked or stamped ''Unclassified'' unless it is essential to convey to a recipient of such material that it has been examined with a view to imposing a security classification and that it has been determined that it does not require classification. However, the marking ''Unclassified'' may be applied to formerly classified material.

§159a.32 Specific markings on documents.

(a) *Overall and Page Marking.* Except as otherwise specified for working papers, the overall classification of a document, whether or not permanently bound, or any copy or reproduction thereof, shall be conspicuously marked, stamped or affixed permanently at the top and bottom on the outside of the front cover (if any), on the title page (if any), on the first page, and on the outside of the back cover (if any). Each interior page, except those that are blank, shall be marked top and bottom according to its content, to include ''Unclassified'' when no classified information is contained on such a page. Alternatively, the overall classification of the document may be conspicuously marked or stamped at the top and bottom of each interior page when such marking is necessary to achieve production efficiency and the particular information to which classification is assigned is otherwise sufficiently identified consistent with the intent of paragraph (c) of §159a.32. In any case, the classification marking of a page shall not supplant the classification marking of portions paragraph (c) of this section of the page marked with lower levels of classification.

(b) *Marking Components.* The major components of some complex documents are likely to be used separately. In such instances, each major component shall be marked as a separate document in accordance with §159a.31. Examples include each annex, appendix, or similar component of a plan, program, or operations order; attachments and appendices to a memorandum or letter; and each major part of a report. If an entire major component is unclassified, the first page of the component may be marked at the top and bottom with the designation ''UNCLASSIFIED'' and a statement included, such as, ''All portions of this (annex, appendix, etc.) are UNCLASSIFIED.'' When this method of marking is used, no further markings are required on the unclassified major component.

(c) *Portion Marking.* (1) Each section, part, paragraph, or similar portion of a classified document shall be marked to show the level of classification of the information contained in or revealed by it, or that it is unclassified. Portions of documents shall be marked in a manner that eliminates doubt as to which of its portions contains or reveals classified information. Classification levels of portions of a document, except as provided in paragraph (e) of this section, shall be shown by the appropriate classification symbol placed immediately following the portion's letter or number, or in the absence of letters or numbers, immediately before the beginning of the portion. In marking sections, parts, paragraphs, or similar portions, the parenthetical symbols ''(TS)'' for Top Secret, ''(S)'' for Secret, ''(C)'' for Confidential, and ''(U)'' for unclassified, shall be used. When appropriate, the symbols ''RD'' for Restricted Data and ''FRD'' for Formerly Restricted Data shall be added, for example, ''(S–RD)'' or ''(C–

FRD).'' In addition, portions that contain Critical Nuclear Weapon Design Information (CNWDI) will be marked ''(N)'' following the classification, for example, ''(S–RD)(N).''

(2) Portion marking of DoD documents containing foreign government information shall be in accordance with §159a.77(d).

(3) Illustrations, photographs, figures, graphs, drawings, charts and similar portions of classified documents will be clearly marked to show their classification or unclassified status. Such markings shall not be abbreviated and shall be prominent and placed within or contiguous to the portion. Captions of such portions shall be marked on the basis of their content alone by placing the symbol ''(TS),'' ''(S),'' ''(C),'' or ''(U)'' immediately preceding the caption.

(4) If, in an exceptional situation, parenthetical portion marking is determined to be impracticable, the document shall contain a statement sufficient to identify the information that is classified and the level of such classification. Thus, for example, each portion of a classified document need not be marked separately if all portions are classified at the same level, provided a statement to that effect is included in the document. In the case of classified compilations, the explanations required by paragraph (d) of this section meet this requirement.

(5) When elements of information in one portion require different classifications, but segregation into separate portions would destroy continuity or context, the highest classification required for any item shall be applied to that portion or paragraph.

(6) Waivers of the foregoing portion marking requirements may be granted for good cause. Any request by a DoD Component senior official for a waiver of portion marking requirements shall be submitted to the DUSD(P) and include the following:

(i) Identification of the information or class of documents for which such waiver is sought;

(ii) Detailed explanation of why the waiver should be granted;

(iii) The Component's judgment of the anticipated dissemination of the information or class of documents for which the waiver is sought, and

(iv) The extent to which such information subject to the waiver may be a basis for derivative classification. Waivers shall be granted only upon a written determination by the DUSD(P) as the designee of the Secretary of Defense, that there will be minimal circulation of the specified documents or information, and minimal potential usage of these documents or information as a source for derivative classification determinations; or there is some other basis to conclude that the benefits of portion marking are clearly outweighed by the increased administrative burdens. The granting and revocation of portion marking waivers shall be reported to the Director of the ISOO by the DUSD(P).

(d) *Compilations*—(1) *Documents.* When classification is required to protect a compilation of unclassified information pursuant to §159a.15(1), the overall classification assigned to such documents shall be placed conspicuously at the top and bottom of each page and on the outside of the front and back covers, if any, and an explanation of the basis for the assigned classification shall be included on the document or on its text.

(2) *Portions of Documents.* If a classified document contains particular portions that are unclassified when standing alone, but classified information will be revealed when they are combined or associated, those portions shall be marked as unclassified, the page shall be marked with the highest classification of any information on or revealed by the page, and an explanation shall be added to the page, or to the document, to explain the classification of the combination or association to the holder. This method of marking also may be used if classified portions on a page, or within a document, will reveal information of a higher classification when they are combined or associated than when they are standing alone.

(e) *Subjects and Titles of Documents.* Subjects or titles of classified documents shall be marked with the appropriate symbol, ''(TS),'' ''(S),'' ''(C),'' or ''(U)'' placed immediately following

and to the right of the item. When applicable, other appropriate symbols, for example, ''(RD)'' or ''(FRD),'' shall be added. (Subjects or titles of documents should be unclassified, if possible.)

(f) *File, Folder, or Group of Documents.* When a file, folder, or group of classified documents is removed from secure storage it shall be marked conspicuously with the highest classification of any classified document included therein or shall have an appropriate classified document cover sheet affixed.

(g) *Transmittal Documents.* A transmittal document, including endorsements and comments when such endorsements and comments are added to the basic communication, shall carry on its face a prominent notation of the highest classification of the information transmitted by it, and a legend showing the classification, if any, of the transmittal document, endorsement, or comment standing alone. For example, an unclassified document that transmits as an attachment a classified document shall bear a notation substantially as follows: ''UNCLASSIFIED WHEN SEPARATED FROM CLASSIFIED ENCLOSURE.''

(h) *Electronically Transmitted Messages.* (1) The copy of a classified message (for example, DD Form 173, Joint Messageform) approved for electronic transmission and maintained as the record copy shall be marked as required by § 159a.31(d) for other documents. Additionally, copies not electronically transmitted (such as, mail and courier copies) shall be marked as required by § 159a.31(d).

(2) The first item of information in the text of a classified electronically transmitted message shall be its overall classification. Paper copies of classified electronically transmitted messages shall be marked at the top and bottom with the assigned classification. Portions shall be marked as prescribed herein for paper copies of documents. When such messages are printed by an automated system, classification markings may be applied by that system, provided that page markings so applied are clearly distinguishable on the face of the document from the printed text.

(3) The originator of a classified electronically transmitted message shall be considered the accountable classifier under § 159a.15(a). The highest level official identified on the message as the sender or, in the absence of such identification, the head of the organization originating the message, is deemed to be the classifier of the message. Thus, a ''Classified by'' line is not required on such messages. The originator is responsible for maintaining adequate records as required by § 159a.31(d)(2) to show the source of an assigned derivative classification.

(4) The last line of text of a classified electronically transmitted message shall show the date or event for downgrading, if appropriate, and the date or event for automatic declassification or ''Originating Agency's Determination Required,'' by abbreviated markings from § 159a.34. The foregoing is not required for messages that contain information identified as Restricted Data or Formerly Restricted Data.

(5) Any document, the classification of which is based solely upon the classification of the content of a classified electronically transmitted message, shall cite the message on the ''Classified by'' line of the newly created document.

(i) *Translations.* Translations of U.S. classified information into a language other than English shall be marked to show the United States as the country of origin, with the appropriate U.S. classification markings and the foreign language equivalent thereof (see Appendix A to this part).

§ 159a.33 Markings on special categories of material.

(a) *General Provisions.* Security classification and applicable associated markings (see § 159a.31(d) and § 159a.33(k)) assigned by the classifier shall be conspicuously stamped, printed, written, painted, or affixed by means of a tag, sticker, decal, or similar device, on classified material other than paper copies of documents, and on containers of such material, if possible. If marking the material or container is not practicable, written notification of

the security classification and applicable associated markings shall be furnished to recipients. The following procedures for marking various kinds of materials containing classified information are not all inclusive and may be varied to accommodate the physical characteristics of the material containing the classified information and to accommodate organizational and operational requirements.

(b) *Charts, Maps, and Drawings.* Charts, maps, and drawings shall bear the appropriate classification marking for the legend, title, or scale blocks in a manner that differentiates between the overall classification of the document and the classification of the legend or title itself. The higher of these markings shall be inscribed at the top and bottom of each such document. When folding or rolling charts, maps, or drawings would cover the classification markings, additional markings shall be applied that are clearly visible when the document is folded or rolled. Applicable associated markings shall be included in or near the legend, title, or scale blocks.

(c) *Photographs, Films, and Recordings.* Photographs, films (including negatives), recordings, and their containers shall be marked to assure that a recipient or viewer will know that classified information of a specified level of classification is involved.

(1) *Photographs.* Negatives and positives shall be marked, whenever practicable, with the appropriate classification designation and applicable associated markings. Roll negatives or positives may be so marked at the beginning and end of each strip. Negatives and positives shall be kept in containers bearing conspicuous classification markings. All prints and reproductions shall be conspicuously marked with the appropriate classification designation and applicable associated markings on the face side of the print if possible. When such markings cannot be applied to the face side, they may be stamped on the reverse side or affixed by pressure tape label, stapled strip, or other comparable means.

NOTE: When self-processing film or paper is used to photograph or reproduce classified information, all parts of the last exposure shall be removed from the camera and destroyed as classified waste, or the camera shall be protected as classified.

(2) *Transparencies and Slides.* Applicable classification markings shall be shown clearly in the image area of each transparency or slide, if possible. In the case of a 35mm or a similar size transparency or slide where the classification markings are not conspicuous unless projected on a screen, for example, the classification markings also shall be marked on its border, holder, or frame. Duplicate classification markings in image areas and on borders, holders, or frames are required if there is any doubt that the image area markings are not conspicuous enough to be seen when the transparencies or slides are not being projected. Other applicable associated markings shall be shown in the image area, or on the border, holder, or frame, or in accompanying documention. It is not necessary that each transparency or slide of a set of transparencies or slides bear applicable associated markings when the set is controlled as a single document. In such cases, the first transparency or slide shall bear the applicable associated markings.

(3) *Motion Picture Films and Video Tapes.* Classified motion picture films and video tapes shall be marked at the beginning and end by titles bearing the appropriate classification markings. Applicable associated markings shall be included at the beginning of such films or tapes. All such marking shall be visible when projected. Reels and cassettes shall be marked with the appropriate classification and kept in containers bearing conspicuous classification and applicable associated markings.

(4) *Recordings.* Sound, magnetic, or electronic recordings shall contain at the beginning and end a clear statement of the assigned classification that will provide adequate assurance that any listener or viewer will know that classified information of a specified level is involved. Recordings shall be kept in containers or on reels that bear conspicuous classification and applicable associated markings.

(5) *Microforms.* Microforms are images, usually produced photographically on transparent or opaque materials, in sizes too small to be read by

the unaided eye. Accordingly, the assigned security classification and abbreviated applicable associated markings shall be conspicuously marked on the microform medium or its container, so as to be readable by the unaided eye. These markings shall also be included on the image so that when the image is enlarged and displayed or printed, the markings will be conspicuous and readable. Such marking will be accomplished as appropriate for the particular microform involved. For example, roll film microforms (or roll microfilm employing 16, 35, 70, or 105 mm films) may generally be marked as provided for roll motion picture film in §159a.33(c)(3) and decks of ''aperture cards'' may be marked as provided in §159a.33(d) for decks of automatic data processing punched cards. Whenever possible, microfiche, microfilm strips, and microform chips shall be marked in accordance with this paragraph.

(d) *Decks of ADP Punched Cards.* When a deck of classified ADP punched cards is handled and controlled as a single document, only the first and last card require classification markings. An additional card shall be added (or the job control card modified) to identify the contents of the deck and the highest classification therein. Such additional card shall include applicable associated markings. Cards removed for separate processing or use and not immediately returned to the deck shall be protected to prevent compromise of any classified information contained therein, and for this purpose shall be marked individually as prescribed in §159a.32(a).

(e) *Removable ADP and Word Processing Storage Media*—(1) *External.* Removable information storage media and devices, used with ADP systems and typewriters or word processing systems, shall bear external markings clearly indicating the classification of the information and applicable associated markings. Included are media and devices that store information recorded in analog or digital form and that are generally mounted or removed by the users or operators. Examples include magnetic tape reels, cartridges, and cassettes; removable discs, disc cartridges, disc packs and diskettes; paper tape reels; and magnetic cards.

(2) *Internal.* ADP systems and word processing systems employing such media shall provide for internal classification marking to assure that classified information contained therein that is reproduced or generated, will bear applicable classification and associated markings. An exception may be made by the DoD Component head, or designee, for the purpose of exempting existing word processing systems when the internal classification and applicable associated markings cannot be implemented without extensive system modification, provided procedures are established to ensure that users and recipients of the media, or the information therein, are clearly advised of the applicable classification and associated markings. For ADP systems, exceptions may be authorized by the DoD Component Designated Approving Authority or Authorities, designated under DoD Directive 5200.28. For purposes of these exemption provisions, ''existing systems'' means word processing and ADP systems already acquired, or, in the case of associated automated information systems, those for which the life cycle management process has already progressed beyond the ''definition/design'' phase as set forth in DoD Directive 7920.1[11]. Requirements for the security of nonremovable ADP storage media and clearance or declassification procedures for various ADP storage media are contained in DoD 5200.28–M[12].

(f) *Documents Produced by ADP Equipment.* The first page, and the front and back covers, if any, of documents produced by ADP equipment shall be marked as prescribed in §159a.32(a). Interior pages also shall be marked as prescribed in §159a.32(a) except that the classification markings of interior pages of fan-folded printouts may be applied by the ADP equipment. When the application of associated markings prescribed by §159a.31(d) by the ADP equipment is not consistent with economical and efficient use of such equipment, such markings may be applied to a document produced by ADP equipment by superimposing upon the first

[11] See footnote 1 to §159a.3.

[12] See footnote 7 to §159a.16(g)(1).

page of such document a ''Notice of Declassification Instructions and Other Associated Markings.'' Such notice shall include the date or event for declassification or the notation ''Originating Agency's Determination Required'' or ''OADR'' and all other such applicable markings. If individual pages of a document produced by ADP equipment are removed or reproduced for distribution to other users, each such page or group of pages shall be marked as prescribed in §159a.31(d) or by superimposing upon each such page or group of pages, a copy of any ''Notice of Declassification Instructions and Other Associated Markings'' applicable to such page or group of pages.

(g) *Material for Training Purposes.* In using unclassified documents or material to simulate classified documents or material for training purposes, such documents or material shall be marked clearly to indicate the actual unclassified status of the information, for example, ''(insert classification designation) for training; otherwise unclassified'' or ''UNCLASSIFIED SAMPLE.''

(h) *Miscellaneous Material.* Documents and material such as rejected copy, typewriter ribbons, carbons, and similar items developed in connection with the handling, processing, production, and of use classified information shall be handled in a manner that assures adequate protection of the classified information involved and destruction at the earliest practicable time (see §159a.32). Unless a requirement exists to retain this material or documents for a specific purpose, there is no need to mark, stamp, or otherwise indicate that the information is classified.

(i) *Special Access Program Documents and Material.* Additional markings as prescribed in directives, regulations and instructions relating to an approved Special Access Program shall be applied to documents and material containing information subject to the special access program. Such additional markings shall not serve as the sole basis for continuing classification of the documents or material to which the markings have been applied. When appropriate, such markings shall be excised to ease timely declassification, downgrading, or removal of the information from special control procedures.

(j) *Secure Telecommunications and Information Handling Equipment.* Applicable classification or Controlled Cryptographic Item (CCI) markings shall be applied to secure telecommunications and information handling equipment or associated cryptographic components. Safeguarding and control procedures for classified and CCI equipment and for safeguarding COMSEC facilities are contained in DoD Instruction 5230.22[12a], National Communications Security Committee (NCSC) Policy Directive 6, DoD Directive C–5200.5[13], National Telecommunications and Information Systems Security Instruction 4001, and National COMSEC Instruction 4003, 4006, and 4008.

(k) *Associated Markings.* Other applicable associated markings required for documents by §159a.31(d) shall be accomplished as prescribed in this section or in any other appropriate manner.

§159a.34 Classification authority, duration, and change in classification markings.

(a) *Declassification and Regrading Marking Procedures.* When classified information is downgraded or declassified in accordance with the assigned downgrading or declassification markings, such markings shall be a sufficient notation of the authority for such action. Whenever classified information is downgraded or declassified earlier than originally scheduled, or upgraded, the material shall be marked promptly and conspicuously to indicate the change, the authority for the action, the date of the action and the identity of the person taking the action. In addition, except for upgrading (see paragraph (d) of this section), prior classification markings shall be canceled, if practicable, but in any event those on the cover (if any) and first page shall be canceled, and the new classification markings, if any, shall be substituted.

(b) *Applying Derivative Declassification Dates.* (1) New material that derives its

[12a] See footnote 1 to §159a.3.

[13] Classified document. Not releasable to the public.

classification from information classified on or after August 1, 1982, shall be marked with the declassification date, event, or the notation ''Originating Agency's Determination Required'' or ''OADR'' assigned to the source information.

(2) New material that derives its classification from information classified prior to August 1, 1982, shall be treated as follows:

(i) If the source material bears a declassification date or event, that date or event shall be carried forward to the new material;

(ii) If the source material bears no declassification date or event, or bears an indeterminate date or event such as ''Upon Notification by Originator,'' ''Cannot Be Determined,'' or ''Impossible to Determine,'' or is marked for declassification review, the new material shall be marked with the notation ''Originating Agency's Determination Required'' or ''OADR''; or

(iii) If the source material is foreign government information bearing no date or event for declassification or is marked for declassification review, the new material shall be marked with the notation ''Originating Agency's Determination Required'' or ''OADR.''

(3) New material that derives its classification from a classification guide issued prior to August 1, 1982, that has not been updated to conform with this Regulation shall be treated as follows:

(i) If the guide specifies a declassification date or event, that date or event shall be applied to the new material; or

(ii) If the guide specifies a declassification review date, the notation ''Originating Agency's Determination Required'' or ''OADR'' shall be applied to the new material.

(c) *Commonly Used Markings.* Each classified document is marked on its face with one or more of the following markings:

(1) *Original Classification.* The following markings are used in original classification § 159a.31(d)(1):

Classified by (See Note 1)
Declassify on (See Note 2)
Message Abbreviation:
DECL (See Note 3)

(2) *Derivative Classification.* The following markings are used in derivative classification § 159a.31(d)(2):

Classified by (See Note 4)
Declassify on (See Note 5)
Message Abbreviation:
DECL (See Note 3)

(3) *Downgrading.* The following marking is used to specify a downgrading § 159a.31(d) (1) and (2):

Downgrade to on (See Note 6)
Message Abbreviation:
DNG/ / (See Note 7)

NOTE 1: Insert identification (position title) of the original classification authority. This line may be omitted if the original classification authority is also the signer or approver of the document.

NOTE 2: Insert the specific date, an event certain to occur, or the notation ''Originating Agency's Determination Required'' or ''OADR.''

NOTE 3: Insert day, month, and year for declassification, for example, ''6 Jun 90,'' an event certain to occur, or ''OADR.''

NOTE 4: Insert identity of the single security classification guide, source document, or other authority for the classification. If more than one such source is applicable, insert the phrase ''Multiple Sources.''

NOTE 5: Insert the specific date or event for declassification or the notation ''Originating Agency's Determination Required'' or ''OADR.'' When multiple sources are used, either the most remote date or event for declassification marked on the sources or, if present on any source, the notation ''Originating Agency's Determination Required'' or ''OADR'' is applied to the new document.

NOTE 6: Insert Secret or Confidential and specific date or event, for example, ''Downgrade to *CONFIDENTIAL* on *6 July 1988*.''

NOTE 7: Insert ''S'' or ''C'' to indicate the downgraded classification and specific date or event, for example, ''DNG/C/6 Jun 87.''

(4) There is no requirement for adding declassification instructions on documents with Restricted Data or Formerly Restricted Data markings (see § 159a.31(b)(3) and § 159a.35 (a) and (b)). Except for electronically transmitted messages, only a completed ''Classified by'' line is added to documents so marked.

(5) Electronically transmitted messages do not require a ''classified by'' line (See § 159a.32(h)(3)).

(6) DoD 5200.1–PH provides additional marking guidance.

(d) *Upgrading.* When material is upgraded it shall be promptly and conspicuously marked as prescribed in paragraph (a) of this section except that in all such cases the old classification markings shall be canceled and new markings substituted.

(e) *Limited Use of Posted Notice for Large Quantities of Material.* (1) When the volume of material is such that prompt remarking of each classified item cannot be accomplished without unduly interfering with operations, the custodian may attach downgrading and declassification notices to the storage unit instead of the remarking required by paragraph (a) of this section. Each notice shall specify the authority for the downgrading or declassification action, the date of the action, and the storage unit to which it applies.

(2) When individual documents or materials are permanently withdrawn from storage units, they shall be remarked promptly as prescribed by paragraph (a) of this section. However, when documents or materials subject to a downgrading or declassification notice are withdrawn from one storage unit solely for transfer to another, or a storage unit containing such documents or materials is transferred from one place to another, the transfer may be made without remarking if the notice is attached to or remains with each shipment.

§ 159a.35 Additional warning notices.

(a) *General Provisions.* (1) In addition to the marking requirements prescribed in § 159a.31(d), the warning notices prescribed in this section shall be displayed prominently on classified documents or materials, when applicable. In the case of documents, these warning notices shall be marked conspicuously on the outside of the front cover, or on the first page if there is no front cover. Transmittal documents, including those that are unclassified (§ 159a.35(g)), also shall bear these additional warning notices, when applicable. In addition, abbreviated forms of the notices set forth in § 159a.35(a), (b), and (c) shall be included in portion markings, as applicable. Further, the warning notice in paragraph (d) of this section, in its short form, shall be included at least once on interior pages, as applicable.

(2) When display of warning notices on other materials is not possible, their applicability to the information shall be included in the written notification of the assigned classification.

(b) *Restricted Data.* Classified documents or material containing Restricted Data as defined in the Atomic Energy Act of 1954, as amended shall be marked as follows:

RESTRICTED DATA

This material contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure subject to administrative and criminal sanctions.

(c) *Formerly Restricted Data.* Classified documents or material containing Formerly Restricted Data, as defined in section 142.d, Atomic Energy Act of 1954, as amended, but no Restricted Data, shall be marked as follows:

FORMERLY RESTRICTED DATA

Unauthorized disclosure subject to administrative and criminal sanctions. Handle as Restricted Data in foreign dissemination. Section 144.b, Atomic Energy Act, 1954.

(d) *Intelligence Sources or Methods Information.* (1) Documents that contain information relating to intelligence sources or methods shall include the following marking unless otherwise proscribed by DoD Instruction 5230.22:

WARNING NOTICE—INTELLIGENCE SOURCES OR METHODS INVOLVED

(2) Existing stamps or preprinted labels containing the caveat ''Warning Notice—Intelligence Sources and Methods Involved'' may be used on documents created on or after the effective date of this part until replacement is required. Any replacement or additional stamps or labels purchased after the effective date of this part shall conform to the wording of paragraph (d)(1) of this section.

(e) *COMSEC Material.* Before release to contractors, COMSEC documents will indicate on the title page, or first page if no title page exists, the following notation:

COMSEC Material—Access by Contractor Personnel Restricted to U.S. Citizens Holding Final Government Clearance.

This notation shall be placed on COMSEC documents or material when originated and when release to contractors can be anticipated. Other COMSEC documents or material shall be marked in accordance with National COMSEC Instruction (NACSI) 4003. Foreign dissemination of COMSEC information is governed by NCSC Policy Directive 6.

(f) *Dissemination and Reproduction Notice.* Classified information that the DoD originator has determined to be subject to special dissemination or reproduction limitations as outlined in §159a.54(1) shall include, as applicable, a statement or statements on its cover sheet, first page, or in the text, substantially as follows:

Reproduction requires approval of originator or higher DoD authority.

Further dissemination only as directed by (insert appropriate office or official) or higher DoD authority.

(g) *Other Notations.* Other notations of restrictions on reproduction, dissemination or extraction of classified information may be used as authorized by DoD Directive C–5200.5, DoD Instruction 5230.22, DoD Directive 5210.2[14], DoD Directive 5100.55[15], DoD Directive 5200.30, Joint Army-Navy-Air Force Publication 119, DoD Directive 5230.24, and NACSI 4003.

§159a.36 Remarking old material.

(a) *General.* (1) Documents and material classified under E.O. 12065 and predecessor E.O.s that are marked for automatic downgrading or automatic declassification on a specific date or event shall be downgraded and declassified pursuant to such markings. Declassification instructions on such documents or material need not be restated to conform with §159a.32(c). (See also §159a.34(a)). Information extracted from these documents or material for use in new documents or material shall be marked for declassification on the date specified in accordance with §159a.31(d)(2).

(2) Documents and material classified under DoD C–5105.21–M–1[16] and predecessor E.O.s that are not marked for automatic downgrading or automatic declassification on a specific date or event shall not be downgraded or declassified without authorization of the originator. Declassification instructions on such documents or material need not be restated to conform with §159a.32(a). Information extracted from these documents or material for use in new documents or material shall be marked for declassification upon the determination of the originator, that is, the ''Declassify on'' line shall be completed with the notation ''Originating Agency's Determination Required'' or ''OADR'' in accordance with §159a.31(d)(2).

(b) *Earlier Declassification and Extension of Classification.* Nothing in this section shall be construed to preclude declassification under subpart D of this part or subsequent extension of classification under §159a.16(c).

Subpart F—Safekeeping and Storage

§159a.37 Storage and storage equipment.

(a) *General Policy.* Classified information shall be stored only under conditions adequate to prevent unauthorized persons from gaining access. The requirements specified in this part represent the minimum acceptable security standards. DoD policy concerning the use of force for the protection of property or information is specified in DoD Directive 5210.56[17]

(b) *Standards for Storage Equipment.* The GSA establishes and publishes minimum standards, specifications, and supply schedules for containers, vault doors, alarm systems, and associated security devices suitable for the storage and protection of classified information. Heads of DoD Components may establish additional controls to prevent unauthorized access. Security filing cabinets conforming to Federal specifications bear a Test Certification Label on the locking drawer, attesting to the security capabilities of the container and lock. (On some older cabinets the label was affixed on the inside of the locked drawer compartment). Cabinets manufactured after February

[14] See footnote 1 to §159a.3.
[15] See footnote 1 to §159a.3.
[16] See footnote 13 to §159a.33(j).
[17] See footnote 1 to §159a.3.

1962 indicate ''General Services Administration Approved Security Container'' on the outside of the top drawer.

(c) *Storage of Classified Information.* Classified information that is not under the personal control and observation of an authorized person, will be guarded or stored in a locked security container as prescribed in the following:

(1) *Top Secret.* Top Secret information shall be stored in:

(i) A safe-type steel file container having a built-in, three-position, dial-type combination lock approved by the GSA or a Class A vault or vault type room that meets the standards established by the head of the DoD Component concerned. When located in buildings, structural enclosures, or other areas not under U.S. Government control, the storage container, vault, or vault-type room must be protected by an alarm system or guarded during nonoperating hours.

(ii) An alarmed area, provided such facilities are adjudged by the local responsible official to afford protection equal to or better than that prescribed in paragraph (c)(1) (i) of this section. When an alarmed area is used for the storage of Top Secret material, the physical barrier must be adequate to prevent:

(A) Surreptitious removal of the material, and

(B) Observation that would result in the compromise of the material. The physical barrier must be such that forcible attack will give evidence of attempted entry into the area. The alarm system must provide immediate notice to a security force of attempted entry. Under field conditions, the field commander will prescribe the measures deemed adequate to meet the storage standards contained in paragraphs (c)(1)(i) and (ii) of this section.

(2) *Secret and Confidential.* Secret and Confidential information shall be stored in the manner prescribed for Top Secret; or in a Class B vault, or a vault-type room, strong room, or secure storage room that meets the standards prescribed by the head of the DoD Component; or, until phased out, in a steel filing cabinet having a built-in, three-position, dial type combination lock; or, as a last resort, an existing steel filing cabinet equipped with a steel lock bar, provided it is secured by a GSA-approved changeable combination padlock. In this latter instance, the keeper or keepers and staples must be secured to the cabinet by welding, rivets, or peened bolts and DoD Components must prescribe supplementary controls to prevent unauthorized access.

(3) *Specialized Security Equipment*—(i) *Field Safe and One-drawer Container.* One-drawer field safes, and GSA approved security containers are used primarily for storage of classified information in the field and in transportable assemblages. Such containers must be securely fastened or guarded to prevent their theft.

(ii) *Map and Plan File.* A GSA-approved map and plan file has been developed for storage of odd-sized items such as computer cards, maps, and charts.

(4) *Other Storage Requirements.* Storage areas for bulky material containing classified information, other than Top Secret, shall have access openings secured by GSA-approved changeable combination padlocks (Federal specification FF–P110 series) or key-operated padlocks with high security cylinders (exposed shackle, military specification P–43951 series, or shrouded shackle, military specification P–43607 series).

(i) When combination padlocks are used, the provisions of paragraph (e) of this section apply.

(ii) When key-operated high security padlocks are used, keys shall be controlled as classified information with classification equal to that of the information being protected and:

(A) A key and lock custodian shall be appointed to ensure proper custody and handling of keys and locks;

(B) A key and lock control register shall be maintained to identify keys for each lock and their current location and custody;

(C) Keys and locks shall be audited each month;

(D) Keys shall be inventoried with each change of custodian;

(E) Keys shall not be removed from the premises;

(F) Keys and spare locks shall be protected in a secure container;

(G) Locks shall be changed or rotated at least annually, and shall be replaced upon loss or compromise of their keys; and

(H) Master keying is prohibited.

(d) *Procurement and Phase-In of New Storage Equipment*—(1) *Preliminary Survey.* DoD activities shall not procure new storage equipment until:

(i) A current survey has been made of on-hand security storage equipment and classified records; and

(ii) Based upon the survey, it has been determined that it is not feasible to use available equipment or to retire, return, declassify or destroy enough records on hand to make the needed security storage space available.

(2) *Purchase of New Storage Equipment.* New security storage equipment shall be procured from those items listed on the GSA Federal Supply Schedule. Exceptions may be made by heads of DoD Components, with notification to the DUSD(P).

(3) Nothing in this subpart shall be construed to modify existing Federal Supply Class Management Assignments made under DoD Directive 5030.47.[18]

(e) *Designations and Combinations*—(1) *Numbering and Designating Storage Facilities.* There shall be no external mark as to the level of classified information authorized to be stored therein. For identification purposes each vault or container shall bear externally an assigned number or symbol.

(2) *Combinations to Containers*—(i) *Changing.* Combinations to security containers shall be changed only by individuals having that responsibility and an appropriate security clearance. Combinations shall be changed:

(A) When placed in use;

(B) Whenever an individual knowing the combination no longer requires access;

(C) When the combination has been subject to possible compromise;

(D) At least annually; or

(E) When taken out of service. Built-in combination locks shall be reset to the standard combination 50–25–50; combination padlocks shall be reset to the standard combination 10–20–30.

(ii) *Classifying Combinations.* The combination of a vault or container used for the storage of classified information shall be assigned a security classification equal to the highest category of the classified information authorized to be stored therein.

(iii) *Recording Storage Facility Data.* A record shall be maintained for each vault, secure room, or container used for storing classified information, showing location of the container, the names, home addresses, and home telephone numbers of the individuals having knowledge of the combination. Standard Form 700, ''Security Container Information'' shall be used for this purpose. (Use of this Standard Form is required when existing supplies of similar purpose forms are exhausted or by September 30, 1986, whichever occurs earlier).

(iv) *Dissemination.* Access to the combination of a vault or container used for the storage of classified information shall be granted only to those individuals who are authorized access to the classified information stored therein.

(3) *Electrically Actuated Locks.* Electricially actuated locks (for example, cypher and magnetic strip card locks) do not afford the required degree of protection of classified information and may not be used as a substitute for the locks prescribed in paragraph (c) of this section.

(f) *Repair of Damaged Security Containers.* Neutralization of lock-outs or repair of any damage that affects the integrity of a security container approved for storage of classified information shall be accomplished only by authorized persons who are cleared or continuously escorted while so engaged.

(1) A GSA-approved security container is considered to have been restored to its original state of security integrity if:

(i) All damaged or altered parts (for example, locking drawer, and drawer head) are replaced; or

(ii) When a container has been drilled immediately adjacent to or through the dial ring to neutralize a lock-out, the replacement lock is equal to the original equipment, and the drilled

[18] See footnote 1 to § 159a.3.

hole is repaired with a tapered, hardened tool-steel pin, or a steel dowel, drill bit, or bearing with a diameter slightly larger than the hole and of such length that when driven into the hole there shall remain at each end of the rod a shallow recess not less than ⅛ inch nor more than 3⁄16 inch deep to permit the acceptance of substantial welds, and the rod is welded both on the inside and outside surfaces. The outside of the drawer head shall then be puttied, sanded, and repainted in such a way that no visible evidence of the hole or its repair remains on the outer surface after replacement of the damaged parts (for example, new lock).

(2) GSA-approved containers that have been drilled in a location or repaired in a manner other than as described in paragraph (f)(1) of this section, will not be considered to have been restored to their original state of security integrity. The Test Certification Label on the inside of the locking drawer and the ''General Services Administration Approved Security Container'' label, if any, on the outside of the top drawer shall be removed from such containers.

(3) If damage to a GSA-approved security container is repaired with welds, rivets, or bolts that cannot be removed and replaced without leaving evidence of entry, the cabinet is limited thereafter to the storage of Secret and Confidential material.

(4) If the damage is repaired using methods other than those permitted in paragraphs (f) (1) and (3) of this section, use of the container will be limited to unclassified material and a notice to this effect will be permanently marked on the front of the container.

§ 159a.38 Custodial precautions.

(a) *Responsibilities of Custodians.* (1) Custodians of classified information shall be responsible for providing protection and accountability for such information at all times and for locking classified information in appropriate security equipment whenever it is not in use or under direct supervision of authorized persons. Custodians shall follow procedures that ensure that unauthorized persons do not gain access to classified information.

(2) Only the head of a DoD Component, or single designee at the headquarters and major command levels, may authorize removal of classified information from designated working areas in off-duty hours, for work at home or otherwise, provided that a GSA-approved security container is furnished and appropriate regulations otherwise provide for the maximum protection possible under the circumstances. (See also §159a.55.) Any such arrangements approved before the effective date of this part shall be reevaluated and, if continued approval is warranted, compliance with this paragraph is necessary.

(b) *Care During Working Hours.* DoD personnel shall take precaution to prevent unauthorized access to classified information.

(1) Classified documents removed from storage shall be kept under constant surveillance and face down or covered when not in use. Cover sheets shall be Standard Forms 703, 704, and 705 for, respectively, Top Secret, Secret, and Confidential documents. (Use of these Standard Forms is required when existing supplies of similar purpose forms are exhausted or by September 30, 1986, whichever occurs earlier).

(2) Preliminary drafts, carbon sheets, plates, stencils, stenographic notes, worksheets, typewriter ribbons, and other items containing classified information shall be either destroyed immediately after they have served their purpose; or shall be given the same classification and secure handling as the classified information they contain.

(3) Destruction of typewriter ribbons from which classified information can be obtained shall be accomplished in the manner prescribed for classified working papers of the same classification. After the upper and lower sections have been cycled through and overprinted five times in all ribbon or typing positions, fabric ribbons may be treated as unclassified regardless of their classified use thereafter. Carbon and plastic typewriter ribbons and carbon paper that have been used in the production of classified information shall be destroyed in the manner prescribed for working papers of the same

classification after initial usage. However, any ribbon in a typewriter that uses technology which enables the ribbon to be struck several times in the same area before it moves to the next position may be treated as unclassified.

(c) *End-of-Day Security Checks.* Heads of activities that process or store classified information shall establish a system of security checks at the close of each working day to ensure that the area is secure; Standard Form 701, ''Activity Security Checklist'' shall be used to record such checks. An integral part of the security check system shall be the securing of all vaults, secure rooms, and containers used for the storage of classified material; Standard Form 702, ''Security Container Check Sheet'' shall be used to record such actions. In addition, Standard Forms 701 and 702 shall be annotated to reflect after-hours, weekend, and holiday activity. (Use of these Standard Forms is required when existing supplies of similar purpose forms are exhausted or by September 30, 1986, whichever occurs earlier).

(d) *Emergency Planning.* (1) Plans shall be developed for the protection, removal, or destruction of classified material in case of fire, natural disaster, civil disturbance, terrorist activities, or enemy action. Such plans shall establish detailed procedures and responsibilities for the protection of classified material to ensure that the material does not come into the possession of unauthorized persons. These plans shall include the treatment of classified information located in foreign countries.

(2) These emergency planning procedures do not apply to material related to COMSEC. Planning for the emergency protection including emergency destruction under no-notice conditions of classified COMSEC material shall be developed in accordance with the requirements of NSA KAG I–D.

(3) Emergency plans shall provide for the protection of classified material in a manner that will minimize the risk of injury or loss of life to personnel. In the case of fire or natural disaster, the immediate placement of authorized personnel around the affected area, preinstructed and trained to prevent the removal of classified material by unauthorized personnel, is an acceptable means of protecting classified material and reducing casualty risk. Such plans shall provide for emergency destruction to preclude capture of classified material when determined to be required. This determination shall be based on an overall commonsense evaluation of the following factors:

(i) Level and sensitivity of classified material held by the activity;

(ii) Proximity of land-based commands to hostile or potentially hostile forces or to communist-controlled countries;

(iii) Flight schedules or ship deployments in the proximity of hostile or potentially hostile forces or near communist-controlled countries;

(iv) Size and armament of land-based commands and ships;

(v) Sensitivity of operational assignment; and

(vi) Potential for aggressive action of hostile forces.

(4) When preparing emergency destruction plans, consideration shall be given to the following:

(i) Reduction of the amount of classified material held by a command as the initial step toward planning for emergency destruction;

(ii) Storage of less frequently used classified material at more secure commands in the same geographical area (if available);

(iii) Transfer of as much retained classified material to microforms as possible, thereby reducing the bulk that needs to be evacuated or destroyed;

(iv) Emphasis on the priorities for destruction, designation of personnel responsible for destruction, and the designation of places and methods of destruction. Additionally, if any destruction site or any particular piece of destruction equipment is to be used by more than one activity or entity, the order or priority for use of the site or equipment must be clearly delineated;

(v) Identification of the individual who is authorized to make the final determination when emergency destruction is to begin and the means by which this determination is to be communicated to all subordinate elements maintaining classified information;

(vi) Authorization for the senior individual present in an assigned space containing classified material to deviate from established plans when circumstances warrant; and

(vii) Emphasis on the importance of beginning destruction sufficiently early to preclude loss of material. The effect of premature destruction is considered inconsequential when measured against the possibility of compromise.

(5) The emergency plan shall require that classified material holdings be assigned a priority for emergency evacuation or destruction. Priorities should be based upon the potential effect on national security should such holdings fall into hostile hands, in accordance with the following general guidelines:

(i) *Priority One.* Exceptionally grave damage (Top Secret material);

(ii) *Priority Two.* Serious damage (Secret material); and

(iii) *Priority Three.* Damage (Confidential material).

(6) If, as determined by appropriate threat analysis, Priority One material cannot otherwise be afforded a reasonable degree of protection from hostile elements in a no-notice emergency situation, provisions shall be made for installation of Anticompromise Emergency Destruct (ACED) equipment to ensure timely initiation and positive destruction of such material[a] in accordance with the following standard: ''With due regard for personnel and structural safety, the ACED system shall reach a stage in destruction sequences at which positive destruction is irreversible within 60 minutes at shore installations, 30 minutes in ships, and 3 minutes in aircraft following activation of the ACED system.''[b]

(7) An ACED requirement is presumed to exist and provisions shall be made for an ACED system to protect Priority One material in the following environments:

(i) Shore-based activities located in or within 50 miles of potentially hostile countries, or located within or adjacent to countries with unstable governments;

(ii) Reconnaissance aircraft, both manned and unmanned, that operate within JCS-designated reconnaissance reporting areas (see Memorandum by the Secretary, Joint Chiefs of Staff (SM) 701–76, Volume II, ''Peacetime Reconnaissance and Certain Sensitive Operations'';[c]

(iii) Naval surface noncombatant vessels operating in hostile areas when not accompanied by a combatant vessel;

(iv) Naval subsurface vessels operating in hostile areas; and

(v) U.S. Navy Special Project ships (Military Sealift Command-operated) operating in hostile areas.

(8) Except in the most extraordinary circumstances, ACED is not applicable to commands and activities located within the United States. Should there be reason to believe that an ACED requirement exists in environments other than in those listed in paragraph (d)(7) of this section, a threat and vulnerability study should be prepared and submitted to the head of the DoD Component concerned or his designee for approval. The threat and vulnerability study should include, at a minimum, the following data, classified if appropriate:

(i) Volume and type of Priority One material held by the activity, that is, paper products, microforms, magnetic tape, and circuit boards.

(ii) A statement certifying that the amount of Priority One material held by the activity has been reduced to the lowest possible level;

(iii) An estimate of the time, beyond the time frames cited above, required to initiate irreversible destruction of

[a] Technological limitations, particularly as to personnel and structural safety, place constraints on the amount of material that can be accommodated in buildings, ships, and aircraft by current ACED systems; therefore, only Priority One material reasonably can be so protected at this time. Nevertheless, after processing Priority One material in an emergency situation involving possible loss to hostile forces, it is imperative that Priority Two material and then Priority Three material be destroyed insofar as is possible by whatever means available.

[b] The time frames indicated above are those for the initiation of irreversible destruction, not necessarily for the completion of such destruction.

[c] SM 701–76 is available on a strict need-to-know basis from the Chief, Documents Division, Joint Secretariat, OJCS.

Priority One material held by the activity, and the methods by which destruction of that material would be attempted in the absence of an ACED system;

(iv) Size and composition of the activity;

(v) Location of the activity and the degree of control it, or other United States authority, exercises over security; and

(vi) Proximity to potentially hostile forces and potential for aggressive action by such forces.

(9) When a requirement is believed to exist for ACED equipment not in the GSA or DoD inventories, the potential requirement shall be submitted to the DUSD(P) for validation in accordance with subsection V. B. of DoD Directive 3224.3[19,d].

(10) In determining the method of destruction of other than Priority One material, any method specified for routine destruction or any other means that will ensure positive destruction of the material may be used. Ideally, any destruction method should provide for early attainment of a point at which the destruction process is irreversible. Additionally, classified material may be jettisoned at sea to prevent its easy capture. It should be recognized that such disposal may not prevent recovery of the material. Where none of the methods previously mentioned can be employed, the use of other means, such as dousing the classified material with a flammable liquid and igniting it, or putting to use the facility garbage grinders, sewage treatment plants, and boilers should be considered.

(11) Under emergency destruction conditions, destruction equipment may be operated at maximum capacity and without regard to pollution, preventive maintenance, and other constraints that might otherwise be observed.

(12) Commands and activities that are required to maintain an ACED system pursuant to paragraph (d)(7) of this section, shall conduct drills periodically to ensure that responsible personnel are familiar with the emergency plan. Such drills should be used to evaluate the anticipated effectiveness of the plan and the prescribed equipment and should be the basis for improvements in planning and equipment use. Actual destruction should not be initiated during drills.

(e) *Telecommunications Conversations.* Classified information shall not be discussed in telephone conversations except as authorized over approved secure communications circuits, that is, cryptographically protected circuits or protected distribution systems installed in accordance with National COMSEC Instruction 4009.

(f) *Security of Meetings and Conferences.* Security requirements and procedures governing disclosure of classified information at conferences, symposia, conventions, and similar meetings, and those governing the sponsorship and attendance of U.S. and foreign personnel at such meetings, are set forth in DoD Directive 5200.12[20], DoD Instruction 5230.20[21], DoD 5220.22–R, and DoD 5220.22–M.

(g) *Safeguarding of U.S. Classified Information Located in Foreign Countries.* Except for classified information that has been authorized for release to a foreign government or international organization pursuant to DoD Directive 5230.11[22], and is under the security control of such government or organization, the retention of U.S. classified material in foreign countries may be authorized only when that material is necessary to satisfy specific U.S. Government requirements. This includes classified material temporarily transferred into a foreign country via U.S. Government personnel authorized to escort or handcarry such material pursuant to §159a.59, as applicable. Whether permanently or temporarily retained, the classified materials shall be stored under U.S. Government control as follows:

(1) At a U.S. military installation, or a location where the United States enjoys extraterritorial status, such as an embassy or consulate.

(2) At a U.S. Government activity located in a building used exclusively by

[19] See footnote 1 to §159a.3.

[d] Information on ACED systems may be obtained from the Office of the Chief of Naval Operations (OP–09N), Navy Department, Washington, DC 20350.

[20] See footnote 1 to §159a.3.

[21] See footnote 1 to §159a.3.

[22] See footnote 1 to §159a.3.

U.S. Government tenants, provided the building is under 24-hour control by U.S. Government personnel.

(3) At a U.S. Government activity located in a building not used exclusively by U.S. Government tenants nor under host government control, provided the classified material is stored in security containers approved by the GSA and is placed under 24-hour control by U.S. Government personnel.

(4) At a U.S. Government activity located in a building not used exclusively by U.S. Government tenants but which is under host government control, provided the classified material is stored in GSA-approved security containers which are further secured in a locked room or area to which only U.S. personnel have access.

(5) When host government and U.S. personnel are co-located, U.S. classified material that has not been authorized for release to the host government pursuant to DoD Directive 5230.11, shall, to the extent possible, be segregated from releasable classified material to facilitate physical control and prevent inadvertent compromise. However, U.S. classified material that is releasable to the host country need not be subject to the 24-hour U.S. control requirement provided the host government exercises its own control measures over the pertinent areas or containers during non-duty hours.

(6) Foreign nationals shall be escorted while in areas where nonreleasable U.S. classified material is handled or stored. However, when required by operational necessity, foreign nationals may be permitted, during duty hours, unescorted entry to such areas provided the nonreleasable information is properly stored or is under the direct personal supervision and control of cleared U.S. personnel who can prevent unauthorized access.

§ 159a.39 Activity entry and exit inspection program.

(a) *Policy.* (1) Commanders and heads of activities shall establish and maintain an inspection program to deter and detect unauthorized introduction or removal of classified material from DoD owned or leased installations and facilities. This program does not replace existing programs for facility and installation security and law enforcement inspection requirements.

(2) The inspection program shall be implemented in a manner which does not interfere unduly with the performance of assigned missions.

(3) The inspection program shall be implemented in a manner which does not significantly disrupt the ingress and egress of persons who are employees of, or visitors to, defense installations and facilities.

(4) Inspections carried out under this program shall be limited to the extent feasible to areas where classified work is being performed, and cover only persons employed within, or visiting, such areas.

(5) Inspections carried out under this program shall be performed at a sufficient frequency to provide a credible deterrent to those who would be inclined to remove classified materials without authority from the installation or facility in question.

(6) The method and frequency of such inspections at a given installation or facility is at the discretion of the commander or head of the installation or facility, or other designated official. Such inspections shall conform to the procedures set forth in the following:

(i) *Inspection Frequency.* (A) Inspections may be aperiodic, that is, at irregular intervals.

(B) Inspections may be accomplished at one or more designated entry/exit points; they need not be carried out at all entry/exit points at the same time.

(C) Inspections may be done on a random basis using any standard which may be appropriate, for example, every third person; every tenth person; every hundredth person, at the entry/exit point(s) designated.

(D) Inspections at a particular entry/exit point(s) may be limited as appropriate to various periods of time, for example, one week, one day, or one hour.

(E) Inspections shall be conducted at all entry/exit points after normal duty hours, including weekends and holidays, on a continuous basis, if practicable.

(b) *Inspection Procedures and Identification.* (1) Inspections shall be limited to that which is necessary to determine whether classified material is

contained in briefcases, shoulder or handbags, luggage, athletic bags, packages, or other similar containers being removed from or taken into the premises. Inspections shall not be done of wallets, change purses, clothing, cosmetic cases, or other objects of an unusually personal nature.

(2) DoD Components shall provide employees who have a legitimate need to remove classified material from the installation or activity with written or printed authorizations to pass through designated entry/exit points. (See § 159a.59(f)) This may include:

(i) The authorization statements prescribed in § 159a.59.

(ii) If authorized in Component instructions, wallet-size cards which describe in general terms the purpose(s) for authorizing the employee to remove classified material from the facility (for example, use at meetings or transmission to authorized recipients).

(3) Inspectors are to ensure that personnel are not removing classified material without authorization. Where inspectors determine that individuals do not appear to have appropriate authorization to remove classified material, they shall request such individual to obtain appropriate authorization before exiting the premises. If, due to the circumstances, this is not feasible, the inspector should attempt to verify by telephone the authority of the individual in question to remove the classified material with the employing office. When such verification cannot be obtained, and if removal cannot be prevented, the inspector shall advise the employing office and appropriate security office as soon as feasible that classified material was removed by the named individual at a particular time and without apparent authorization.

(4) If the employing office determines that classified material was removed by one of its employees without authority, it shall request an investigation of the circumstances of the removal by appropriate investigative authorities. Where such investigation confirms a violation of security procedures, other than espionage or deliberate compromise, for which § 159a.50 applies, appropriate administrative, disciplinary, or legal action shall be taken.

Subpart G—Compromise of Classified Information

§ 159a.41 Policy.

Compromise of classified information presents a threat to the national security. Once a compromise is known to have occurred, the seriousness of damage to U.S. interests must be determined and appropriate measures taken to negate or minimize the adverse effect of such compromise. When possible, action also should be taken to regain custody of the documents or material that were compromised. In all cases, however, appropriate action must be taken to identify the source and reason for the compromise and remedial action taken to ensure further compromises do not occur. The provisions of DoD Instruction 5240.4[23] and DoD Directive 5210.50[24] apply to compromises covered by this subpart.

§ 159a.42 Cryptographic and sensitive compartmented information.

(a) The procedures for handling compromises of cryptographic information are set forth in NACSI 4006 and implementing instructions.

(b) The procedures for handling compromises of SCI information are set forth in DoD TS–5105.21–M–2[25] and DoD C–5105.21–M–1[26].

§ 159a.43 Responsibility of discoverer.

(a) Any person who has knowledge of the loss or possible compromise of classified information shall immediately report such fact to the security manager of the person's activity (see § 159a.93(e)) or to the commanding officer or head of the activity in the security manager's absence.

(b) Any person who discovers classified information out of proper control shall take custody of such information and safeguard it in an appropriate manner, and shall notify immediately an appropriate security authority.

[23] See footnote 1 to § 159a.3.

[24] See footnote 1 to § 159a.3.

[25] See footnote 13 to § 159a.33(j).

[26] See footnote 13 to § 159a.33(j).

§ 159a.44 Preliminary inquiry.

The immediate commander, supervisor, security manager, or other authority shall initiate a preliminary inquiry to determine the circumstances surrounding the loss or possible compromise of classified information. The preliminary inquiry shall establish one of the following:

(a) That a loss or compromise of classified information did not occur;

(b) That a loss or compromise of classified information did occur but the compromise reasonably could not be expected to cause damage to the national security. If, in such instances, the official finds no indication of significant security weakness, the report of preliminary inquiry will be sufficient to resolve the incident and, when appropriate, support the administrative sanctions under § 159a.98; or

(c) That the loss or compromise of classified information did occur and that the compromise reasonably could be expected to cause damage to the national security or that the probability of damage to the national security cannot be discounted. Upon this determination, the responsible official shall:

(1) Report the circumstances of the compromise to an appropriate authority as specified in DoD Component instructions;

(2) If the responsible official is the originator, take the action prescribed in § 159a.47; and

(3) If the responsible official is not the originator, notify the originator of the known details of the compromise, including identification of the classified information. If the originator is unknown, notification will be sent to the office specified in DoD Component instructions.

§ 159a.45 Investigation.

If it is determined that further investigation is warranted, such investigation will include the following:

(a) Identification of the source, date, and circumstances of the compromise.

(b) Complete description and classification of each item of classified information compromised;

(c) A thorough search for the classified information;

(d) Identification of any person or procedure responsible for the compromise. Any person so identified shall be apprised of the nature and circumstances of the compromise and be provided an opportunity to reply to the violation charged. If such person does not choose to make a statement, this fact shall be included in the report of investigation;

(e) An analysis and statement of the known or probable damage to the national security that has resulted or may result (See § 159a.15(k)), and the cause of the loss or compromise; or a statement that compromise did not occur or that there is minimal risk of damage to the national security;

(f) An assessment of the possible advantage to foreign powers resulting from the compromise; and

(g) A compilation of the data in paragraphs (a) through (f) of this section, in a report to the authority ordering the investigation to include an assessment of appropriate corrective, administrative, disciplinary, or legal actions. (Also see § 159a.100).

§ 159a.46 Responsibility of authority ordering investigation.

(a) The report of investigation shall be reviewed to ensure compliance with this part and instructions issued by DoD Components.

(b) The recommendations contained in the report of investigation shall be reviewed to determine sufficiency of remedial, administrative, disciplinary, or legal action proposed and, if adequate, the report of investigation shall be forwarded with recommendations through supervisory channels (See § 159a.98 and § 159a.99).

(c) Whenever an action is contemplated against any person believed responsible for the compromise of classified information, damage assessments shall be coordinated with the legal counsel of the DoD Component where the individual responsible is assigned or employed. Whenever a violation of criminal law appears to have occurred and a criminal prosecution is contemplated, the DoD Component responsible for the damage assessment shall apprise the General Counsel, Department of Defense. See § 159a.101.

§ 159a.47 Responsibility of originator.

The originator or an official higher in the originator's supervisory chain shall, upon receipt of notification of loss or probable compromise of classified information, take action as prescribed in § 159a.15(k).

§ 159a.48 System of control of damage assessments.

Each DoD Component shall establish a system of controls and internal procedures to ensure that damage assessments are conducted when required and that records are maintained in a manner that facilitates their retrieval and use within the Component.

§ 159a.49 Compromises involving more than one agency.

(a) Whenever a compromise involves the classified information or interests of more than one DoD Component or other agency, each such activity undertaking a damage assessment shall advise the others of the circumstances and findings that affect their information and interests. Whenever a damage assessment incorporating the product of two or more DoD Components or other agencies is needed, the affected activities shall agree upon the assignment of responsibility for the assessment.

(b) Whenever a compromise of U.S. classified information is the result of actions taken by foreign nationals, by foreign government officials, or by U.S. nationals employed by international organizations, the activity performing the damage assessment shall ensure, through appropriate intergovernmental liaison channels, that information pertinent to the assessment is obtained. Whenever more than one activity is responsible for the assessment, those activities shall coordinate the request prior to transmittal through appropriate channels.

§ 159a.50 Espionage and deliberate compromise.

Cases of espionage and deliberate unauthorized disclosure of classified information to the public shall be reported in accordance with DoD Instruction 5240.4 and DoD Directive 5210.50 and implementing issuances.

§ 159a.51 Unauthorized absentees.

When an individual who has had access to classified information is on unauthorized absence, an inquiry as appropriate under the circumstances, to include consideration of the length of absence and the degree of sensitivity of the classified information involved, shall be conducted to detect if there are any indications of activities, behavior, or associations that may be inimical to the interest of national security. When such indications are detected, a report shall be made to the DoD Component counterintelligence organization.

Subpart H—Access, Dissemination, and Accountability

§ 159a.53 Access.

(a) *Policy.* (1) Except as otherwise provided for in paragraph (c) of this section, no person may have access to classified information unless that person has been determined to be trustworthy and unless access is essential to the accomplishment of lawful and authorized Government purposes, that is, the person has the appropriate security clearance and a need-to-know. Further, cleared personnel may not have access until they have been given an initial security briefing (see § 159a.70). Procedures shall be established by the head of each DoD Component to prevent unnecessary access to classified information. There shall be a demonstrable need for access to classified information before a request for a personnel security clearance can be initiated. The number of people cleared and granted access to classified information shall be maintained at the minimum number that is consistent with operational requirements and needs. No one has a right to have access to classified information solely by virtue of rank or position. The final responsibility for determining whether an individual's official duties require possession of or access to any element or item of classified information, and whether the individual has been granted the appropriate security clearance by proper authority, rests upon the individual who has authorized possession, knowledge, or control of the information and not upon

the prospective recipient. These principles are equally applicable if the prospective recipient is a DoD Component, including commands and activities, other Federal agencies, DoD contractors, foreign governments, and others.

(2) Because of the extreme importance to the national security of Top Secret information and information controlled within approved Special Access Programs, employees shall not be permitted to work alone in areas where such information is in use or stored and accessible by those employees. This general policy is an extra safeguarding measure for the nation's most vital classified information and it is not intended to cast doubt on the integrity of DoD employees. The policy does not apply in those situations where one employee with access is left alone for brief periods during normal duty hours. When compelling operational requirements indicate the need, DoD Component heads may waive this requirement in specific, limited cases. This waiver authority may be delegated to the senior official (§ 159a.93 (b) and (c)) of the DoD Component who may redelegate the authority but only if so authorized by the head of the DoD Component. (Any waiver should include provisions for periodically ensuring the health and welfare of individuals left alone in vaults or secure areas).

(b) *Access by Persons Outside the Executive Branch.* Classified information may be made available to individuals or agencies outside the Executive Branch provided that such information is necessary for performance of a function from which the Government will derive a benefit or advantage, and that such release is not prohibited by the originating department or agency. Heads of DoD Components shall designate appropriate officials to determine, before the release of classified information, the propriety of such action in the interest of national security and assurance of the recipient's trustworthiness and need-to-know.

(1) *Congress.* Access to classified information or material by Congress, its committees, members, and staff representatives shall be in accordance with DoD Directive 5400.4[27]. Any DoD employee testifying before a congressional committee in executive session in relation to a classified matter shall obtain the assurance of the committee that individuals present have a security clearance commensurate with the highest classification of the information that may be discussed. Members of Congress, by virtue of their elected positions, are not investigated or cleared by the Department of Defense.

(2) *Government Printing Office (GPO).* Documents and material of all classifications may be processed by the GPO, which protects the information in accordance with the DoD/GPO Security Agreement of February 20, 1981.

(3) *Representatives of the General Accounting Office (GAO).* Representatives of the GAO may be granted access to classified information originated by and in possession of the Department of Defense when such information is relevant to the performance of the statutory responsibilities of that office, as set forth in DoD Directive 7650.1[28]. Officials of the GAO, as designated in Appendix B to this part, are authorized to certify security clearances, and the basis therefor. Certifications will be made by these officials pursuant to arrangements with the DoD Component concerned. Personal recognition or presentation of official GAO credential cards are acceptable for identification purposes.

(4) *Industrial, Educational, and Commercial Entities.* (i) Bidders, contractors, grantees, educational, scientific or industrial organizations may have access to classified information only when such access is essential to a function that is necessary in the interest of the national security, and the recipients are cleared in accordance with DoD 5220.22–R.

(ii) Contractor employees whose duties do not require access to classified information are not eligible for personnel security clearance and cannot be investigated under the DISP. In exceptional situations, when a military command is vulnerable to sabotage and its mission is of critical importance to national security, National Agency

[27] See footnote 1 to § 159a.3.
[28] See footnote 1 to § 159a.3.

Checks may be conducted on such individuals with the approval of the DUSD(P).

(5) *Historical Researchers.* Persons outside the Executive Branch who are engaged in historical research projects may be authorized access to classified information provided that an authorized official within the DoD Component with classification jurisdiction over the information:

(i) Makes a written determination that such access is clearly consistent with the interests of national security in view of the intended use of the material to which access is granted by certifying that the requester has been found to be trustworthy pursuant to paragraph (a)(1) of this section;

(ii) Limits such access to specific categories of information over which that DoD Component has classification jurisdiction and to any other category of information for which the researcher obtains the written consent of a DoD Component or non-DoD department or agency that has classification jurisdiction over information contained in or revealed by documents within the scope of the proposed historical research;

(iii) Maintains custody of the classified material at a DoD installation or activity or authorizes access to documents in the custody of the NARA;

(iv) Obtains the researcher's agreement to safeguard the information and to submit any notes and manuscript for review by all DoD Components or non-DoD departments or agencies with classification jurisdiction for a determination that no classified information is contained therein by execution of a statement entitled, ''Conditions Governing Access to Official Records for Historical Research Purposes''; and

(v) Issues an authorization for access valid for not more than 2 years from the date of issuance that may be renewed under regulations of the issuing DoD Component.

(6) *Former Presidential Appointees.* Persons who previously occupied policy making positions to which they were appointed by the President may not remove classified information upon departure from office as all such material must remain under the security control of the U.S. Government. Such persons may be authorized access to classified information that they originated, received, reviewed, signed, or that was addressed to them while serving as such an appointee, provided that an authorized official within the DoD Component with classification jurisdiction for such information:

(i) Makes a written determination that such access is clearly consistent with the interests of national security in view of the intended use of the material to which access is granted and by certifying that the requester has been found to be trustworthy pursuant to paragraph (a)(1) of this section;

(ii) Limits such access to specific categories of information over which that DoD Component has classification jurisdiction and to any other category of information for which the former appointee obtains the written consent of a DoD Component or non-DoD department or agency that has classification jurisdiction over information contained in or revealed by documents with the scope of the proposed access;

(iii) Retains custody of the classified material at a DoD installation or activity or authorizes access to documents in the custody of the National Archives and Records Service; and

(iv) Obtains the former presidential appointee's agreement to safeguard the information and to submit any notes and manuscript for review by all DoD Components or non-DoD departments or agencies with classification jurisdiction for a determination that no classified information is contained therein.

(7) *Judicial Proceedings.* DoD Directive 5405.2[29] governs the release of classified information in litigation.

(c) *Access by Foreign Nationals, Foreign Governments, and International Organizations.* (1) Classified information may be released to foreign nationals, foreign governments, and international organizations only when authorized under the provisions of the National Disclosure Policy and DoD Directive 5230.11; and

(2) Access to COMSEC information by foreign persons and activities shall be in accordance with policy issuances of the National Telecommunications and

[29] See footnote 1 to § 159a.3.

Information Systems Security Committee (NTISSC).

(d) *Other Situations.* When necessary in the interests of national security, heads of DoD Components, or their single designee, may authorize access by persons outside the Federal government, other than those enumerated in paragraphs (b) and (c) of this section, to classified information upon determining that the recipient is trustworthy for the purpose of accomplishing a national security objective; and that the recipient can and will safeguard the information from unauthorized disclosure.

(e) *Access Required by Other Executive Branch Investigative and Law Enforcement Agents.* (1) Normally, investigative agents of other departments or agencies may obtain access to DoD information through established liaison or investigative channels.

(2) When the urgency or delicacy of a Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), or Secret Service investigation precludes use of established liaison or investigative channels, FBI, DEA, or Secret Service agents may obtain access to DoD information as required. However, this information shall be protected as required by its classification. Before any public release of the information so obtained the approval of the head of the activity or higher authority shall be obtained.

(f) *Access by Visitors.* Procedures shall be established to control access to classified information by visitors. (DoD Instruction 5230.20 provides further guidance regarding foreign visitors.)

(1) Except when a continuing, frequent working relationship is established, through which current security clearance and need-to-know are determined, DoD personnel visiting other activities of the Department of Defense, its contractors, and other agencies shall provide advance notification of the pending visit that establishes the visitor's security clearance and the purpose of the visit. Visit requests shall be signed by an official other than the visitor who is in a position to verify the visitor's security clearance.

(2) Visit requests normally should include the following:

(i) Full name, date and place of birth, social security number, and rank or grade of visitor;

(ii) Security clearance of the visitor;

(iii) Employing activity of the visitor;

(iv) Name and address of activity to be visited;

(v) Date and duration of proposed visit;

(vi) Purpose of visit in sufficient detail to establish need-to-know; and

(vii) Names of persons to be contacted.

(3) Visit requests may remain valid for not more than 1 year.

§ 159a.54 Dissemination.

(a) *Policy.* DoD Components shall establish procedures consistent with this Regulation for the dissemination of classified material. The originating official or activity may prescribe specific restrictions on dissemination of classified information when necessary. (See § 159a.35(f). Particular emphasis shall be placed on traditional need-to-know measures to aid in the strict control of classified information.)

(b) *Restraints on Special Access Requirements.* Special requirements with respect to access, distribution, and protection of classified information shall require prior approval in accordance with subpart M of this part.

(c) *Information Originating in a Non-DoD Department or Agency.* Except under rules established by the Secretary of Defense, or as provided by section 102 of the National Security Act, classified information originating in a department or agency other than Department of Defense shall not be disseminated outside the Department of Defense without the consent of the originating department or agency.

(d) *Foreign Intelligence Information.* Dissemination of foreign intelligence information shall be in accordance with the provisions of DoD Instruction 5230.22 and DoD Directive C–5230.23[30].

(e) *Restricted Data and Formerly Restricted Data.* Information bearing the warning notices prescribed in § 159a.35 (b) and (c) shall not be disseminated outside authorized channels without the consent of the originator. Access to

[30] See footnote 13 to § 159a.33(j).

and dissemination of Restricted Data by DoD personnel shall be subject to DoD Directive 5210.2.

(f) *NATO Information.* Classified information originated by NATO shall be safeguarded in accordance with DoD Directive 5100.55.

(g) *COMSEC Information.* COMSEC information shall be disseminated in accordance with NACSI 4005 and implementing instructions.

(h) *Dissemination of Top Secret Information.* (1) Top Secret information, originated within the Department of Defense, may not be disseminated outside the Department of Defense without the consent of the originating DoD Component, or higher authority.

(2) Top Secret information, whenever segregable from classified portions bearing lower classifications, shall be distributed separately.

(3) Standing distribution requirements for Top Secret information and materials, such as distribution lists, shall be reviewed at least annually to verify the recipients' need-to-know.

(i) *Dissemination of Secret and Confidential Information.* (1) Secret and Confidential information, originated within the Department of Defense, may be disseminated within the Executive Branch, unless prohibited by the originator. (See § 159a.35(f)).

(2) Standing distribution requirements for Secret and Confidential information and materials, such as distribution lists, shall be reviewed at least annually to verify the recipients' need-to-know.

(j) *Code Words, Nicknames, and Exercise Terms.* The use of code words, nicknames, and exercise terms is subject to the provisions of subpart M and Appendix C.

(k) *Scientific and Technical Meetings.* Use of classified information in scientific and technical meetings is subject to the provisions of DoD Directive 5200.12.

(l) *Limited Dissemination (LIMDIS).* This section establishes limits on measures for the protection of information beyond those involving access to classified information per se, but not so stringent as to require the establishment of a Special Access Program. It prohibits use of terminology indicating enhancements to need-to-know, such as Special Need-to-Know (SNTK), MUST KNOW, Controlled Need-to-Know (CNTK), or other similar security upgrade designations and associated unique security requirements such as specialized nondisclosure statements. Limited dissemination controls are the only security enhancement short of a Special Access Program which may be employed for control over specific information for specified periods of time. In this context, these procedures may be initiated and continued on a showing that additional access controls are required in order to assure the security of the designated information. The decision to apply these procedures shall be made at the original classification authority level of command or supervision in accordance with the implementing information security instructions promulgated by the DoD Component. Except by agreement, such requirements shall not be imposed outside of the approving DoD Component. LIMDIS protective measures are restricted to one or more of the following:

(1) Decentralized maintenance of disclosure listings, briefings concerning access limitations, and physical security restrictions limited to requirements such as placing the material in sealed envelopes within approved storage containers to avoid inadvertent disclosure and the commingling with other files;

(2) Using unclassified nicknames (no code words may be assigned to LIMDIS information);

(3) Marking the material as LIMDIS along with the assigned nickname;

(4) Marking inner envelopes containing designated LIMDIS information with the notation: ''To be Opened Only By Personnel Authorized Access'';

(5) Requiring electronically transmitted messages containing designated information to be marked with the uniform caveat LIMDIS; and

(6) Prescribing unique oversight procedures to be accomplished by Component professional security personnel (industrial security inspections will be conducted in the normal manner by the Defense Investigative Service).

§ 159a.55 Accountability and control.

(a) *Top Secret Information.* DoD activities shall establish the following procedures:

(1) *Control Officers.* Top Secret Control Officers (TSCOs) and alternates shall be designated within offices to be responsible for receiving, dispatching, and maintaining accountability registers of Top Secret documents. Such individuals shall be selected on the basis of experience and reliability, and shall have Top Secret security clearances. TSCOs need not be appointed in those instances where there is no likelihood of processing Top Secret documentation.

(2) *Accountability*—(i) *Top Secret Registers.* Top Secret accountability registers shall be maintained by each office originating or receiving Top Secret information. Such registers shall be retained for 2 years and shall, as a minimum, reflect the following:

(A) Sufficient information to identify adequately the Top Secret document or material to include the title or appropriate short title, date of the document, and identification of the originator;

(B) The date the document or material was received;

(C) The number of copies received or later reproduced; and

(D) The disposition of the Top Secret document or material and all copies of such documents or material.

(ii) *Serialization and Copy Numbering.* Top Secret documents and material shall be numbered serially. In addition, each Top Secret document shall be marked to indicate its copy number, for example, copy –1– of –2– copies.

(iii) *Disclosure Records.* Each Top Secret document or item of material shall have appended to it a Top Secret disclosure record. The name and title of all individuals, including stenographic and clerical personnel to whom information in such documents and materials has been disclosed, and the date of such disclosure, shall be recorded thereon. Disclosures to individuals who may have had access to containers in which Top Secret information is stored, or who regularly handle a large volume of such information need not be so recorded. Such individuals, when identified on a roster, are deemed to have had access to such information. Disclosure records shall be retained for 2 years after the documents or materials are transferred, downgraded, or destroyed.

(3) *Inventories.* All Top Secret documents and material shall be inventoried at least once annually. The inventory shall reconcile the Top Secret accountability register with the documents or material on hand. At such time, each document or material shall be examined for completeness. DoD Component senior officials (§ 159a.93 (b) and (c)) may authorize the annual inventory of Top Secret documents and material in repositories, libraries, or activities that store large volumes of Top Secret documents or material to be limited to documents and material to which access has been granted within the past year, and 10 percent of the remaining inventory. If a storage system contains large volumes of information and security measures are adequate to prevent access by unauthorized persons, a request for waiver of the annual inventory requirement accompanied by full justification may be submitted to the DUSD(P).

(4) *Retention.* Top Secret information shall be retained only to the extent necessary to satisfy current requirements. Custodians shall destroy nonrecord copies of Top Secret documents when no longer needed. Record copies of documents that cannot be destroyed shall be reevaluated and, when appropriate, downgraded, declassified, or retired to designated records centers.

(5) *Receipts.* Top Secret documents and material will be accounted for by a continuous chain of receipts. Receipts shall be maintained for 2 years.

(b) *Secret Information.* Administrative procedures shall be established by each DoD Component for controlling Secret information and material originated or received by an activity; distributed or routed to a sub-element of such activity; and disposed of by the activity by transfer of custody or destruction. The control system for Secret information must be determined by a practical balance of security and operating efficiency and must meet the following minimum requirements:

(1) It must provide a means to ensure that Secret material sent outside a

major subordinate element (the activity) of the DoD Component concerned has been delivered to the intended recipient. Such delivery may be presumed where the material is sent electronically over secure voice or data circuits. Ensuring physical delivery may be accomplished by use of a receipt as provided in §159.58(c)(2) or through hand-to-hand transfer when the receiving party acknowledges responsibility for the Secret material.

(2) It must provide a record of receipt and dispatch of Secret material by each major subordinate element. The dispatch record requirement may be satisfied when the distribution of Secret material is evident from addresses or distribution lists for classified documentation. Records of receipt and dispatch are required regardless of the means used to ensure delivery of the material (see paragraph (b)(1) of this section).

(3) Records of receipt and dispatch for Secret material shall be retained for a minimum of 2 years.

(c) *Confidential Information.* Administrative controls shall be established to protect Confidential information received, originated, transmitted, or stored by an activity.

(d) *Receipt of Classified Material.* Procedures shall be developed within DoD activities to protect incoming mail, bulk shipments, and items delivered by messenger until a determination is made whether classified information is contained therein. Screening points shall be established to limit access to classified information to cleared personnel.

(e) *Working Papers.* (1) Working papers are documents and material accumulated or created in the preparation of finished documents and material. Working papers containing classified information shall be:

(i) Dated when created;

(ii) Marked with the highest classification of any information contained therein;

(iii) Protected in accordance with the assigned classification;

(iv) Destroyed when no longer needed; and

(v) Accounted for, controlled, and marked in the manner prescribed for a finished document of the same classification when:

(A) Released by the originator outside the activity or transmitted electrically or through message center channels within the activity;

(B) Retained more than 90 days from date of origin;

(C) Filed permanently; or

(D) Top Secret information is contained therein.

(2) Heads of DoD Components, or their single designees, may approve waivers of accountability, control, and marking requirements for working papers containing Top Secret information for activities within their Components on a case-by-case basis provided a determination is made that:

(i) The conditions set forth in paragraph (e)(1)(v) (A), (B), or (C) of this section, will remain in effect;

(ii) The activity seeking a waiver routinely handles large volumes of Top Secret working papers and compliance with prescribed accountability, control, and marking requirements would have an adverse affect on the activity's mission or operations; and

(iii) Access to areas where Top Secret working papers are handled is restricted to personnel who have an appropriate level of clearance, and other safeguarding measures are adequate to preclude the possibility of unauthorized disclosure.

(3) In all cases in which a waiver is granted under paragraph (e)(2) of this section, the DUSD(P) shall be notified.

(f) *Restraint on Reproduction.* Except for the controlled initial distribution of information processed or received electrically or as provided by §159a.2(f) and §159a.29(c), portions of documents and materials that contain Top Secret information shall not be reproduced without the consent of the originator or higher authority. Any stated prohibition against reproduction shall be observed strictly. (See §159a.35(f)) To the extent possible, DoD Components shall establish classified reproduction facilities where only designated personnel can reproduce classified materials and institute key control systems for reproduction areas. Also, when possible, two people shall be involved in the reproduction process to help assure positive control and safeguarding of all

copies. The following additional measures apply to reproduction equipment and to the reproduction of classified information:

(1) Copying of documents containing classified information shall be minimized;

(2) Officials authorized to approve the reproduction of Top Secret and Secret information shall be designated by position title and shall review the need for reproduction of classified documents and material with a view toward minimizing reproduction.

(3) Specific reproduction equipment shall be designated for the reproduction of classified information. Rules for reproduction of classified information shall be posted on or near the designated equipment;

(4) Notices prohibiting reproduction of classified information shall be posted on equipment used only for the reproduction of unclassified information;

(5) DoD Components shall ensure that equipment used for reproduction of classified information does not leave latent images in the equipment or on other material;

(6) All copies of classified documents reproduced for any purpose including those incorporated in a working paper are subject to the same controls prescribed for the document from which the reproduction is made; and

(7) Records shall be maintained for 2 years to show the number and distribution of reproduced copies of all Top Secret documents, of all classified documents covered by special access programs distributed outside the originating agency, and of all Secret and Confidential documents that are marked with special dissemination and reproduction limitations.

(See §159a.35(f))

Subpart I—Transmission

§159a.57 Methods of transmission or transportation.

(a) *Policy*. Classified information may be transmitted or transported only as specified in this subpart.

(b) *Top Secret Information*. Transmission of Top Secret information shall be effected only by:

(1) The Armed Forces Courier Service (ARFCOS);

(2) Authorized DoD Component Courier Services,

(3) If appropriate, the Department of State Courier System;

(4) Cleared and designated U.S. military personnel and Government civilian employees traveling on a conveyance owned, controlled, or chartered by the U.S. Government or DoD contractors;

(5) Cleared and designated U.S. Military personnel and government civilian employees by surface transportation;

(6) Cleared and designated U.S. Military personnel and government civilian employees on scheduled commercial passenger aircraft within and between the United States, its Territories, and Canada, when approved in accordance with §159a.59(d)(1).

(7) Cleared and designated U.S. Military personnel and government civilian employees on scheduled commercial passenger aircraft on flights outside the United States, its territories, and Canada, when approved in accordance with §159a.59(d)(2).

(8) Cleared and designated DoD contractor employees within and between the United States and its Territories provided that the transmission has been authorized in writing by the appropriate contracting officer or his designated representative, and the designated employees have been briefed on their responsibilities as couriers or escorts for the protection of Top Secret material. Complete guidance for Top Secret transmission is specified in DoD 5220.22–R and DoD 5220.22–M.

(9) A cryptographic system authorized by the Director, NSA, or via a protected distribution system designed and installed to meet the standards included in the National COMSEC and Emanations Security (EMSEC) Issuance System.

(c) *Secret Information*. Transmission of Secret information may be effected by:

(1) Any of the means approved for the transmission of Top Secret information except that Secret information may be introduced into the ARFCOS only when the control of such information cannot be otherwise maintained in U.S. custody. This restriction does not apply to SCI and COMSEC information;

(2) Appropriately cleared contractor employees within and between the United States and its Territories provided that:

(i) The designated employees have been briefed in their responsibilities as couriers or escorts for protecting Secret information;

(ii) The classified information remains under the constant custody and protection of the contractor personnel at all times; and

(iii) The transmission otherwise meets the requirements specified in DoD 5220.22–R and DoD 5220.22–M. In other areas, appropriately cleared DoD contractor employees may transmit classified material only as prescribed by DoD 5220.22–R and DoD 5220.22–M.

(3) U.S. Postal Service registered mail within and between the United States and its Territories;

(4) U.S. Postal Service registered mail through Army, Navy, or Air Force Postal Service facilities outside the United States and its Territories, provided that the information does not at any time pass out of U.S. citizen control and does not pass through a foreign postal system or any foreign inspection;

(5) U.S. Postal Service and Canadian registered mail with registered mail receipt between U.S. Government and Canadian Government installations in the United States and Canada;

(6) Carriers authorized to transport Secret information by way of a Protective Security Service (PSS) under the DoD Industrial Security Program. This method is authorized only within the U.S. boundaries and only when the size, bulk, weight, and nature of the shipment, or escort considerations make the use of other methods impractical. Routings for these shipments will be obtained from the Military Traffic Management Command (MTMC);

(7) The following carriers under appropriate escort: government and government contract vehicles including aircraft, ships of the U.S. Navy, civil service-operated U.S. Naval ships, and ships of U.S. registry. Appropriately cleared operators of vehicles, officers of ships or pilots of aircraft who are U.S. citizens may be designated as escorts provided the control of the carrier is maintained on a 24-hour basis. The escort shall protect the shipment at all times, through personal observation or authorized storage to prevent inspection, tampering, pilferage, or unauthorized access. However, observation of the shipment is not required during the period it is stored in an aircraft or ship in connection with flight or sea transit, provided the shipment is loaded into a compartment that is not accessible to any unauthorized persons or in a specialized secure, safe-like container that is:

(i) Constructed of solid building material that provides a substantial resistance to forced entry;

(ii) Constructed in a manner that precludes surreptitious entry through disassembly or other means, and that attempts at surreptitious entry would be readily discernible through physical evidence of tampering; and

(iii) Secured by a numbered cable seal lock affixed to a substantial metal hasp in a manner that precludes surreptitious removal and provides substantial resistance to forced entry.

(8) Use of specialized containers aboard aircraft requires that:

(i) Appropriately cleared personnel maintain observation of the material as it is being loaded aboard the aircraft and that observation of the aircraft continues until it is airborne;

(ii) Observation by appropriately cleared personnel is maintained at the destination as the material is being off-loaded and at any intermediate stops. Observation will be continuous until custody of the material is assumed by appropriately cleared personnel.

(d) *Confidential Information.* Transmission of Confidential information may be effected by:

(1) Means approved for the transmission of Secret information. However, U.S. Postal Service registered mail shall be used for Confidential only as indicated in paragraph (c)(2) of this section;

(2) U.S. Postal Service registered mail for:

(i) Confidential information of NATO;

(ii) Other Confidential material to and from FPO or APO addressees located outside the United States and its Territories;

(iii) Other addressees when the originator is uncertain that their location is within U.S. boundaries. Use of return postal receipts on a case-by-case basis is authorized.

(3) U.S. Postal Service first class mail between DoD Component locations anywhere in the United States and its Territories. However, the outer envelope or wrappers of such Confidential material shall be endorsed ''POSTMASTER: Address Correction Requested/Do Not Forward.'' Certified or, if appropriate, registered mail shall be used for material directed to DoD contractors and to non-DoD agencies of the Executive Branch. U.S. Postal Service Express Mail Service may be used between DoD Component locations, between DoD contractors, and between DoD Components and DoD contractors.

(4) Within U.S. boundaries, commercial carriers that provide a Constant Surveillance Service (CSS). Information concerning commercial carriers that provide CSS may be obtained from the MTMC.

(5) In the custody of commanders or masters of ships of U.S. registry who are U.S. citizens. Confidential information shipped on ships of U.S. registry may not pass out of U.S. Government control. The commanders or masters must give and receive classified information receipts and agree to:

(i) Deny access to the Confidential material by unauthorized persons, including customs inspections, with the understanding that Confidential cargo that would be subject to customs inspection will not be unloaded; and

(ii) Maintain control of the cargo until a receipt is obtained from an authorized representative of the consignee.

(6) Such alternative or additional methods of transmission as the head of any DoD Component may establish by rule or regulation, provided those methods afford at least an equal degree of security.

(e) *Transmission of Classified Material to Foreign Governments.* After a determination by designated officials pursuant to DoD Directive 5230.11 that classified information or material may be released to a foreign government, the material shall be transferred between authorized representatives of each government in compliance with the provisions of this subpart. To assure compliance, each contract, agreement, or other arrangement that involves the release of classified material to foreign entities shall either contain transmission instructions or require that a separate transportation plan be approved by the appropriate DoD security and transportation officials prior to release of the material. (See DoD TS–5105.21–M–3[31] for guidance regarding SCI.)

(1) Classified material to be released directly to a foreign government representative shall be delivered or transmitted only to a person who has been designated in writing by the recipient government as its officer, agent, or employee (hereafter referred to as the designated representative). Foreign governments may designate a freight forwarder as their agent. This written designation shall contain assurances that such person has a security clearance at the appropriate level and that the person will assume full security responsibility for the material on behalf of the foreign government. The recipient will be required to execute a receipt for the material, regardless of the level of classification.

(2) Classified material that is suitable for transfer by courier or postal service, and which cannot be transferred directly to a foreign government's designated representative as specified in paragraph (e)(1) of this section, shall be transmitted by one of the methods specified in paragraph (b), (c), or (d) of this section, for the designated classification level to:

(i) An embassy, consulate, or other official agency of the recipient government having extraterritorial status in the United States, or to

(ii) A U.S. Embassy or a U.S. military organization in the recipient country or in a third-party country, if applicable, for delivery to a designated representative of the intended recipient government. In either case, the assurance in paragraph (e)(1) of this section, and a receipt, must be obtained.

(3) The shipment of classified material as freight via truck, rail, aircraft,

[31] See footnote 13 to §159a.33(j)

or ship shall be in compliance with the following:

(i) *Shipment Resulting from Foreign Military Sales (FMS).* DoD officials authorized to approve a FMS transaction that involves the delivery of U.S. classified material to a foreign purchaser shall, at the outset of negotiation or consideration of proposal, consult with DoD transportation authorities (Military Traffic Management Command, Military Sealift Command, Military Airlift Command, or other, as appropriate) to determine whether secure shipment from the CONUS point of origin to the ultimate foreign destination is feasible. Normally, the United States will use the Defense Transportation System (DTS) to deliver classified material to the recipient government. If, in the course of FMS case processing, the foreign purchaser proposes to take delivery and custody of the classified material in the United States and use it own facilities and transportation for onward shipment to its territory, the foreign purchaser or its designated representative shall be required to submit a transportation plan for DoD review and approval. This plan, as a minimum, shall specify the storage facilities, delivery and transfer points, carriers, couriers or escorts, and methods of handling to be used from the CONUS point of origin to the final destination and return shipment when applicable. (See Appendix E to this part) Security officials of the DoD Component that initiates the FMS transaction shall evaluate the transportation plan to determine whether the plan adequately ensures protection of the highest level of classified material involved. Unless the DoD Component initiating the FMS transaction approves the transportation plan as submitted, or it is modified to meet U.S. security standards, shipment by other than DTS shall not be permitted. Transmission instructions or the requirement for an approved transportation plan shall be incorporated into the security requirements of the United States Department of Defense Offer and Acceptance (DD Form 1513).

(ii) *Shipments Resulting from Direct Commercial Sales.* Classified shipments resulting from direct commercial sales must comply with the same security standards that apply to FMS shipments. Defense contractors, therefore, will consult, as appropriate, with the purchasing government, the DIS Regional Security Office, and the owning Military Department prior to consummation of a commercial contract that will result in the shipment of classified material to obtain approval of the transportation plan.

(iii) *Delivery within the United States, Its Territories, or Possessions.* Delivery of classified material to a foreign government at a point within the United States, its territories, or its possessions, shall be made only to a person identified in writing by the recipient government as its designated representative as specified in paragraph (e)(1) of this section. The only authorized delivery points are:

(A) An embassy, consulate, or other official agency under the control of the recipient government.

(B) Point of origin. When a designated representative of the recipient government accepts delivery of classified U.S. material at the point of origin (for example, a manufacturing facility or depot), the DoD official who transfers custody shall obtain a receipt for the classified material and assure that the recipient is cognizant or secure means of onward movement of the classified material to its final destination, consistent with the approved transportation plan.

(C) Military or commercial ports of embarkation (POE) that are recognized points of departure from the United States, its territories, or possessions, for onloading aboard a ship, aircraft, or other carrier authorized under paragraph (e)(3)(v) of this section. In these cases, the transportation plan shall provide for U.S.-controlled secure shipment to the CONUS transshipment point and the identification of a secure storage facility, government or commercial, at or in proximity to the POE. A DoD official authorized to transfer custody is to supervise or observe the onloading of FMS material being transported via the DTS and other onloading wherein physical and security custody of the material has yet to be transferred formally to the foreign recipient. In the event that transfer of physical and security custody cannot

be accomplished promptly, the DoD official shall ensure that the classified material is either returned to a secure storage facility of the U.S. shipper (government or contractor); or segregated and placed under constant surveillance of a duly cleared U.S. security force at the POE; or held in the secure storage facility (government or commercial) designated in the transportation plan.

(D) Freight forwarder facility that is identified by the recipient government as its designated representative and that is cleared in accordance with paragraph (e)(3)(vi) of this section, to the level of the classified material to be received. In these cases, a person identified as a designated representative must be present to accept delivery of the classified material and receipt for it, to include full acceptance of security responsibility.

(iv) *Delivery Outside the United States, Its Territories, or Possessions*—(A) *Delivery within the recipient country.* Classified U.S. material to be delivered to a foreign government within the recipient country shall be delivered on arrival in the recipient country to a U.S. Government representative who shall arrange for its transfer to a designated representative of the recipient government. If the shipment is escorted by a U.S. Government official authorized to accomplish the transfer of custody, the material may be delivered directly to the recipient government's designated representative upon arrival.

(B) *Delivery Within a Third Country.* Classified material to be delivered to a foreign government representative within a third country shall be delivered to an agency or installation of the United States, or of the recipient government, that has extraterritorial status or otherwise is exempt from the jurisdiction of the third country. Unless the material is accompanied by a U.S. Government official authorized to accomplish the transfer of custody, a U.S. Government official shall be designated locally to receive the shipment upon arrival and be vested with authority to effect delivery to the intended recipient government's designated representative.

(v) *Overseas Carriers.* Overseas shipments of U.S. classified material shall be made only via ships, aircraft, or other carriers that are:

(A) Owned or chartered by the U.S. Government or under U.S. registry,

(B) Owned or chartered by or under the registry of the recipient government, or

(C) Otherwise expressly authorized by the head of the DoD Component having classification jurisdiction over the material involved. Overseas shipments of classified material shall be escorted, prepared for shipment, packaged, and stored onboard as prescribed elsewhere in this subpart and in DoD 5220.22–R and DoD 5220.22–M.

(vi) *Freight Forwarders.* Only freight forwarders that have been granted an appropriate security clearance by the Department of Defense or the recipient government are eligible to receive, process, and store U.S. classified material authorized for release to foreign governments. However, a freight forwarder that does not have access to or custody of the classified material need not be cleared.

(f) *Consignor-Consignee Responsibility for Shipment of Bulky Material.* The consignor of a bulk shipment shall:

(1) Normally, select a carrier that will provide a single line service from the point of origin to destination, when such a service is available;

(2) Ship packages weighing less than 200 pounds in closed vehicles only;

(3) Notify the consignee, and military transshipping activities, of the nature of the shipment (including level of classification), the means of shipment, the number of seals, if used, and the anticipated time and date of arrival by separate communication at least 24 hours in advance of arrival of the shipment. Advise the first military transshipping activity that, in the event the material does not move on the conveyance originally anticipated, the transshipping activity should so advise the consignee with information of firm transshipping date and estimated time of arrival. Upon receipt of the advance notice of a shipment of classified material, consignees and transshipping activities shall take appropriate steps to receive the classified shipment and to protect it upon arrival.

(4) Annotate the bills of lading to require the carrier to notify the consignor immediately by the fastest means if the shipment is unduly delayed enroute. Such annotations shall not under any circumstances disclose the classified nature of the commodity. When seals are used, annotate substantially as follows:

DO NOT BREAK SEALS EXCEPT IN EMERGENCY OR UPON AUTHORITY OF CONSIGNOR OR CONSIGNEE. IF BROKEN APPLY CARRIER'S SEALS AS SOON AS POSSIBLE AND IMMEDIATELY NOTIFY CONSIGNOR AND CONSIGNEE.

(5) Require the consignee to advise the consignor of any shipment not received more than 48 hours after the estmated time of arrival furnished by the consignor or transshipping activity. Upon receipt of such notice, the consignor shall immediately trace the shipment. If there is evidence that the classified material was subjected to compromise, the procedures set forth in subpart G of this part for reporting compromises shall apply.

(g) *Transmission of COMSEC Information.* COMSEC information shall be transmitted in accordance with National COMSEC Instruction 4005.

(h) *Transmission of Restricted Data.* Restricted Data shall be transmitted in the same manner as other information of the same security classification. The transporting and handling of nuclear weapons or nuclear components shall be in accordance with DoD Directives 4540.1[32] and 5210.41[33] and applicable DoD Component directives and regulations.

[54 FR 26959, June 27, 1989; 54 FR 46610, Nov. 6, 1989]

§ 159a.58 Preparation of material for transmission, shipment, or conveyance.

(a) *Envelopes or Containers.* (1) Whenever classified information is transmitted, it shall be enclosed in two opaque sealed envelopes or simliar wrappings when size permits, except as provided by the following:

(2) Whenever classified material is transmitted of a size not suitable for transmission in accordance with paragraph (a)(1) of this section, it shall be enclosed in two opaque sealed containers, such as boxes or heavy wrappings.

(i) If the classified information is an internal component of a packageable item of equipment, the outside shell or body may be considered as the inner enclosure provided it does not reveal classified information.

(ii) If the classified material is an inaccessible internal component of a bulky item of equipment that is not reasonably packageable, the outside or body of the item may be considered to be a sufficient enclosure provided the shell or body does not reveal classified information.

(iii) If the classified material is an item or equipment that is not reasonably packageable and the shell or body is classified, it shall be concealed with an opaque covering that will hide all classified features.

(iv) Specialized shipping containers, including closed cargo transporters, may be used instead of the above packaging requirements. In such cases, the container may be considered the outer wrapping or cover.

(3) Material used for packaging shall be of such strength and durability as to provide security protection while in transit, prevent items from breaking out of the container, and to facilitate the detection of any tampering with the container. The wrappings shall conceal all classified characteristics.

(4) Closed and locked vehicles, compartments, or cars shall be used for shipments of classified information except when another method is authorized by the consignor. Alternative methods authorized by the consignor must provide security equivalent to or better than the methods specified herein. In all instances, individual packages weighing less than 200 pounds gross shall be shipped only in a closed vehicle.

(5) To minimize the possibility of compromise of classified material caused by improper or inadequate packaging thereof, responsible officials shall ensure that proper wrappings are used for mailable bulky packages. Responsible officials shall require the inspection of bulky packages to determine whether the material is suitable

[32] See footnote 1 to § 159a.3

[33] See footnote 1 to § 159a.3

for mailing or whether it should be transmitted by other approved means.

(6) When classified material is hand-carried outside an activity, a locked briefcase may serve as the outer wrapper. In such cases, the addressing requirements of paragraph (b)(4) of this section do not apply; however, the requirements of paragraph (b)(3) of this section are applicable.

(b) *Addressing.* (1) Classified information shall be addressed to an official government activity or DoD contractor with a facility clearance and not to an individual. This is not intended, however, to prevent use of office code numbers or such phrases in the address as ''Attention: Research Department,'' or similar aids in expediting internal routing, in addition to the organization address.

(2) Classified written information shall be folded or packed in such a manner that the text will not be in direct contact with the inner envelope or container. A receipt form shall be attached to or enclosed in the inner envelope or container for all Secret and Top Secret information; Confidential information will require a receipt only if the originator deems it necessary. The mailing of written materials of different classifications in a single package should be avoided. However, when written materials of different classifications are transmitted in one package, they shall be wrapped in a single inner envelope or container. A receipt listing all classified information for which a receipt is requested shall be attached or enclosed. The inner envelope or container shall be marked with the highest classification of the contents.

(3) The inner envelope or container shall show the address of the receiving activity, classification, including, where appropriate, the ''Restricted Data'' marking, and any applicable special instructions. It shall be carefully sealed to minimize the possibility of access without leaving evidence of tampering.

(4) An outer or single envelope or container shall show the complete and correct address and the return address of the sender.

(5) An outer cover or single envelope or container shall not bear a classification marking, a listing of the contents divulging classified information, or any other unusual data or marks that might invite special attention to the fact that the contents are classified.

(6) Care must be taken to ensure that classified information intended only for U.S. elements of international staffs or other organizations is addressed specifically to those elements.

(c) *Receipt Systems.* (1) Top Secret information shall be transmitted under a chain of receipts covering each individual who gets custody.

(2) Secret information shall be covered by a receipt when transmitted to a foreign government (including foreign government embassies located in the United States) and when transmitted between major subordinate elements of DoD Components and other authorized addressees except that a receipt is not required when there is a hand-to-hand transfer between U.S. personnel and the recipient acknowledges responsibility for the Secret information.

(3) Receipts for Confidential information are not required except when the information is transmitted to a foreign government (including foreign government embassies located in the United States) or upon request.

(4) Receipts shall be provided by the transmitter of the material and the forms shall be attached to the inner cover.

(i) Postcard receipt forms may be used.

(ii) Receipt forms shall be unclassified and contain only such information as is necessary to identify the material being transmitted.

(iii) Receipts shall be retained for at least 2 years.

(5) In those instances where a fly-leaf (page check) form is used with classified publications, the postcard receipt will not be required.

(d) *Exceptions.* Exceptions may be authorized to the requirements contained in this subpart by the head of the Component concerned or designee, provided the exception affords equal protection and accountability to that provided above. Proposed exceptions that do not meet these minimum standards shall be submitted to the DUSD(P) for approval.

§ 159a.59 Restrictions, procedures, and authorization concerning escort or handcarrying of classified information.

(a) *General Restrictions.* Appropriately cleared personnel may be authorized to escort or handcarry classified material between their duty station and an activity to be visited subject to the following conditions:

(1) The storage provisions of § 159a.37 and § 159a.38(g) of subpart F of this part shall apply at all stops enroute to the destination, unless the information is retained in the personal possession and under constant surveillance of the individual at all times. The hand carrying of classified information on trips that involve an overnight stop is not permissible without advance arrangements for proper overnight storage in a U.S. Government facility or, if in the United States, a cleared contractor's facility that has the requisite storage capability.

(2) Classified material shall not be read, studied, displayed, or used in any manner in public conveyances or places.

(3) When classified material is carried in a private, public or government conveyance, it shall not be placed in any detachable storage compartment such as automobile trailers, luggage racks, aircraft travel pods, or drop tanks nor, under any circumstances, left unattended.

(4) Responsible officials shall provide a written statement to all individuals escorting or carrying classified material aboard commercial passenger aircraft authorizing such transmission. This authorization statement may be included in official travel orders and should ordinarily permit the individual to pass through passenger control points without the need for subjecting the classified material to inspection. Specific procedures for carrying classified documents aboard commercial aircraft are contained in paragraph (c) of this section.

(5) Each activity shall list all classified information carried or escorted by traveling personnel. All classified information shall be accounted for.

(6) Individuals authorized to handcarry or escort classified material shall be fully informed of the provisions of this subpart, and shall sign a statement to that effect prior to the issuance of written authorization or identification media. This statement shall be retained for a minimum of 2 years; it need not be executed on each occasion that the individual is authorized to transport classified information provided a signed statement is on file.

(b) *Restrictions on Handcarrying Classified Information Aboard Commercial Passenger Aircraft.* Classified information shall not be hand-carried aboard commercial passenger aircraft unless:

(1) There is neither time nor means available to move the information in the time required to accomplish operational objectives or contract requirements.

(2) The handcarry has been authorized by an appropriate official in accordance with paragraph (d) of this section.

(3) In the case of the handcarry of classified information across international borders, arrangements have been made to ensure that such information will not be opened by customs, border, postal, or other inspectors, either U.S. or foreign.

(4) The handcarry is accomplished aboard a U.S. carrier. Foreign carriers will be utilized only when no U.S. carrier is available and then the approving official must ensure that the information will remain in the custody and physical control of the U.S. escort at all times.

(c) *Procedures for Handcarrying Classified Information Aboard Commercial Passenger Aircraft*—(1) *Basic requirements.* (i) Advance and continued coordination by the DoD activity and contractor officials shall be made with departure airline and terminal officials and, when possible, with intermediate transfer terminals to develop mutually satisfactory arrangements within the terms of this issuance and Federal Aviation Administration (FAA) guidance. Specifically, a determination should be made beforehand whether documentation described in paragraph (c)(4) of this section, will be required. Local FAA Security Officers can be of assistance in making this determination. To aid coordination and planning, a listing of FAA field offices is at Appendix D to this part.

(ii) The individual designated as courier shall be in possession of either DD Form 2, ''Armed (or Uniformed) Services Identification Card'' (any color), or other DoD or contractor picture identification card and written authorization to carry classified information.

(2) *Procedures for carrying classified information in envelopes.* Persons carrying classified information should process through the airline ticketing and boarding procedures the same as all other passengers except for the following:

(i) The classified information being carried shall contain no metal bindings and shall be contained in sealed envelopes. Should such envelopes be contained in a briefcase or other carry-on luggage, the briefcase or luggage shall be routinely offered for opening for inspection for weapons. The screening officials may check envelopes by X-ray machine, flexing, feel, and weight, without opening the envelopes themselves.

(ii) Opening or reading of the classified document by the screening official is not permitted.

(3) *Procedures for transporting classified information in packages.* Classified information in sealed or packaged containers shall be processed as follows:

(i) The government or contractor official who has authorized the transport of the classified information shall notify the appropriate air carrier in advance.

(ii) The passenger carrying the information shall report to the affected airline ticket counter before boarding, present his documentation, and the package or cartons to be exempt from screening. The airline representative will review the documentation and description of the containers to be exempt.

(iii) If satisfied with the identification of the passenger and his documentation, the official will provide the passenger with an escort to the screening station and authorize the screening personnel to exempt the container from physical or other type inspection.

(iv) If the airline official is not satisfied with the identification of the passenger or the authenticity of his documentation, the passenger will not be permitted to board, and not be subject to further screening for boarding purposes.

(v) The actual loading and unloading of the information will be under the supervision of a representative of the air carrier; however, appropriately cleared personnel shall accompany the material and keep it under surveillance during loading and unloading operations. In addition, appropriately cleared personnel must be available to conduct surveillance at any intermediate stops where the cargo compartment is to be opened.

(vi) DoD Components and contractor officials shall establish and maintain appropriate liaison with local FAA officials, airline representatives and airport terminal administrative and security officials. Prior notification is emphasized to ensure that the airline representative can make timely arrangements for courier screening.

(4) *Documentation.* (i) When authorized to carry sealed envelopes or containers containing classified information, both government and contractor personnel shall present an identification card carrying a photograph, descriptive data, and signature of the individual. (If the identification card does not contain date of birth, height, weight, and signature, these items must be included in the written authorization.)

(A) DoD personnel shall present an official identification issued by U.S. Government agency.

(B) Contractor personnel shall present identification issued by the contractor or the U.S. Government. Contractors' identification cards shall carry the name of the employing contractor, or otherwise be marked to denote ''contractor.''

(C) The courier shall have the original of the authorization letter. A reproduced copy is not acceptable; however, the traveler shall have sufficient authenticated copies to provide a copy to each airline involved. The letter shall be prepared on letterhead stationery of the agency or contractor authorizing the carrying of classified material in addition, the letter shall:

(*1*) Give the full name of the individual and his employing agency or company;

(*2*) Describe the type of identification the individual will present (for example, Naval Research Laboratory Identification Card, No. 1234; ABC Corporation Identification Card No. 1234);

(*3*) Describe the material being carried (for example, three sealed packages, 9″ × 8″ × 24″, addressee and addressor);

(*4*) Identify the point of departure, destination, and known transfer points;

(*5*) Carry a date of issue and an expiration date;

(*6*) Carry the name, title, and signature of the official issuing the letter. Each package or carton to be exempt shall be signed on its face by the official who signed the letter; and

(*7*) Carry the name of the government agency designated to confirm the letter of authorization, and its telephone number. The telephone number of the agency designated shall be an official U.S. Government number.

(ii) Information relating to the issuance of DoD identification cards is contained in DoD Instruction 1000.13[34]. The green, gray, and red DD Forms 2 and other DoD and contractor picture ID card are acceptable to FAA.

(iii) The Director, DIS, shall establish standards for the issuance of identification cards when required by contractor employees selected as couriers or whose duties will involve handcarrying of classified material.

(d) *Authority to Approve Escort or Handcarry of Classified Information Aboard Commercial Passenger Aircraft*—(1) *Within the United States, its Territories, and Canada.* (i) DoD Component officials who have been authorized to approve travel orders and designate couriers may approve the escort or handcarry of classified information within the United States, its Territories, and Canada.

(ii) The Director, DIS, may authorize contractor personnel to handcarry classified material in emergency or time-sensitive situations subject to adherence with the procedures and limitations specified in this section.

(2) *Outside the United States, its Territories, and Canada.* The head of a DoD Component, or single designee at the headquarters or major command level, may authorize the escort or handcarrying of classified information outside the area encompassed by the boundaries of the United States, its Territories, and Canada upon certification by the requestor that:

(i) The material is not present at the destination;

(ii) The material is needed urgently for a specified official purpose; and

(iii) There is a specified reason that the material could not be transmitted by other approved means to the destination in sufficient time for the stated purpose.

Subpart J—Disposal and Destruction

§ 159a.61 Policy.

Documentary record information originated or received by a DoD Component in connection with the transaction of public business, and preserved as evidence of the organization, functions, policies, operations, decisions, procedures, or other activities of any U.S. Government department or agency or because of the informational value of the data contained therein, may be disposed of or destroyed only in accordance with DoD Component record management regulations. Nonrecord classified information, and other material of similar temporary nature, shall be destroyed when no longer needed under procedures established by the head of the cognizant DoD Component. These procedures shall incorporate means of verifying the destruction of classified information and material and be consistent with the following requirements.

§ 159a.62 Methods of destruction.

Classified documents and material shall be destroyed by burning or, with the approval of the cognizant DoD Component head or designee, by melting, chemical decomposition, pulping, pulverizing, cross-cut shredding, or mutilation sufficient to preclude recognition or reconstruction of the classified information. (Strip shredders purchased prior to June 1, 1986 may continue to be used but only in circumstances where reconstruction of

[34] See footnote 1 to § 159a.3.

the residue is precluded. Shredding significant amounts of unclassified material together with classified material normally will meet this requirement.)

§ 159a.63 Destruction procedures.

(a) Procedures shall be instituted that ensure all classified information intended for destruction actually is destroyed. Destruction records and imposition of a two-person rule, that is, having two cleared persons involved in the entire destruction process, will satisfy this requirement for Top Secret information. Imposition of a two-person rule, without destruction records, will satisfy this requirement for Secret information, as will use of destruction records without imposition of the two-person rule. Only one cleared person needs to be involved in the destruction process for Confidential information.

(b) When burn bags are used for the collection of classified material that is to be destroyed at central destruction facilities, such bags shall be controlled in a manner designed to minimize the possibility of their unauthorized removal and the unauthorized removal of their classified contents prior to actual destruction. When filled, burn bags shall be sealed in a manner that will facilitate the detection of any tampering with the bag.

(c) Procedures to ensure that all classified information intended for destruction actually is destroyed, other than those in paragraphs (a) and (b) of this section, shall be submitted to the DoD Component's senior official (§ 159a.93(b) and (c)) for approval.

§ 159a.64 Records of destruction.

(a) Records of destruction are required for Top Secret information. The record shall be dated and signed at the time of destruction by two persons cleared for access to Top Secret information. However, in the case of Top Secret information placed in burn bags for central disposal, the destruction record may be signed by the officials when the information is so placed and the bags are sealed. Top Secret burn bags shall be numbered serially and a record kept of all subsequent handling of the bags until they are destroyed. This record may be in lieu of actual burn bag receipts and shall be maintained for a minimum of 2 years.

(b) Records of destruction of Secret and Confidential information are not required except for NATO Secret and some limited categories of specially controlled Secret information. When records of destruction are used for Secret information, only one cleared person has to sign such records. (DoD Directive 5100.55 provides guidance on the destruction of NATO classified material.)

(c) Records of destruction shall be maintained for 2 years.

§ 159a.65 Classified waste.

Waste material, such as handwritten notes, carbon paper, typewriter ribbons, and working papers that contains classified information must be protected to prevent unauthorized disclosure of the information. Classified waste shall be destroyed when no longer needed by a method described in § 159a.62. Destruction records are not required.

§ 159a.66 Classified document retention.

(a) Classified documents that are not permanently valuable records of the government shall not be retained more than 5 years from the date of origin, unless such retention is authorized by and in accordance with DoD Component record disposition schedules.

(b) Throughout the Department of Defense, the head of each activity shall establish at least one clean-out day each year where a portion of the work performed in every office with classified information stored is devoted to the destruction of unneeded classified holdings.

Subpart K—Security Education

§ 159a.68 Responsibility and objectives.

Heads of DoD Components shall establish security education programs for their personnel. Such programs shall stress the objectives of improving the protection of information that requires it. They shall also place emphasis on the balance between the need to

release the maximum information appropriate under the Freedom of Information Act (32 CFR part 285) and the interest of the Government in protecting the national security.

§ 159a.69 Scope and principles.

The security education program shall include all personnel authorized or expected to be authorized access to classified information. Each DoD Component shall design its program to fit the requirements of different groups of personnel. Care must be exercised to assure that the program does not evolve into a perfunctory compliance with formal requirements without achieving the real goals of the program. The program shall, as a minimum, be designed to:

(a) Advise personnel of the adverse effects to the national security that could result from unauthorized disclosure and of their personal, moral, and legal responsibility to protect classified information within their knowledge, possession, or control;

(b) Indoctrinate personnel in the principles, criteria, and procedures for the classification, downgrading, declassification, marking, control and accountability, storage, destruction, and transmission of classified information and material, as prescribed in this Regulation, and alert them to the strict prohibitions against improper use and abuse of the classification system;

(c) Familiarize personnel with procedures for challenging classification descisions believed to be improper;

(d) Familiarize personnel with the security requirements of their particular assignment;

(e) Inform personnel of the techniques employed by foreign intelligence activities in attempting to obtain classified information, and their responsibility to report such attempts;

(f) Advise personnel of the penalties for engaging in espionage activities;

(g) Advise personnel of the strict prohibition against discussing classified information over an unsecure telephone or in any other manner that permits interception by unauthorized persons;

(h) Inform personnel of the penalties for violation or disregard of the provisions of this part (see § 159a.97(b));

(i) Instruct personnel that individuals having knowledge, possession, or control of classified information must determine, before disseminating such information, that the prospective recipient has been cleared for access by competent authority; needs the information in order to perform his or her official duties; and can properly protect (or store) the information.

§ 159a.70 Initial briefings.

DoD personnel granted a security clearance (see §159a.53) shall not be permitted to have access to classified information until they have received an initial security briefing and have signed Standard Form 189, ''Classified Information Nondisclosure Agreement.'' DoD 5200.1–PH–1[35] provides a sample briefing and additional information regarding Standard Form 189. Cleared personnel employed prior to June 1, 1986 must sign Standard Form 189 as soon as practicable but not later than February 28, 1990.

§ 159a.71 Refresher briefings.

Programs shall be established to provide, at a minimum, annual security training for personnel having continued access to classified information. The elements outlined in § 159a.69 shall be tailored to fit the needs of experienced personnel.

§ 159a.72 Foreign travel briefings.

(a) Personnel who have had access to classified information shall be given a foreign travel briefing, before travel, to alert them to their possible exploitation under the following conditions:

(1) Travel to or through communist-controlled countries; and

(2) Attendance at international scientific, technical, engineering or other professional meetings in the United States or in any country outside the United States where it can be anticipated that representatives of Communist-controlled countries will participate or be in attendance. (See also DoD Directive 5240.6[36].)

(b) Individuals who travel frequently, or attend or host meetings of foreign visitors as described in paragraph (a)(2)

[35] See footnote 2 to § 159a.3

[36] See footnote 1 to § 159a.3.

of this section, need not be briefed for each occasion, but shall be provided a thorough briefing at least once every 6 months and a general reminder of security responsibilities before each such activity.

§ 159a.73 Termination briefings.

(a) Upon termination of employment, administrative withdrawal of security clearance, or contemplated absence from duty or employment for 60 days or more, DoD military personnel and civilian employees shall be given a termination briefing, return all classified material, and execute a Security Termination Statement. This statement shall include:

(1) An acknowledgment that the individual has read the appropriate provisions of the Espionage Act, other criminal statutes, DoD regulations applicable to the safeguarding of classified information to which the individual has had access, and understands the implications thereof;

(2) A declaration that the individual no longer has any documents or material containing classified information in his or her possession;

(3) An acknowledgement that the individual will not communicate or transmit classified information to any unauthorized person or agency; and

(4) An acknowledgement that the individual will report without delay to the FBI or the DoD Component concerned any attempt by any unauthorized person to solicit classified information.

(b) When an individual refuses to execute a Security Termination Statement, that fact shall be reported immediately to the security manager of the cognizant organization concerned. In any such case, the individual involved shall be debriefed orally. The fact of a refusal to sign a Security Termination Statement shall be reported to the Director, Defense Investigative Service who shall assure that it is recorded in the Defense Central Index of Investigations.

(c) The security termination statement shall be retained by the DoD Component that authorized the individual access to classified information for the period specified in the Component's record retention schedules, but for a minimum of 2 years after the individual is given a termination briefing.

Subpart L—Foreign Government Information

§ 159a.75 Classification.

(a) *Classification.* (1) Foreign government information classified by a foreign government or international organization of governments shall retain its original classification designation or be assigned a U.S. classification designation that will ensure a degree of protection equivalent to that required by the government or organization that furnished the information. Original classification authority is not required for this purpose.

(2) Foreign government information that was not classified by a foreign entity but was provided with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence must be classified by an original classification authority. The two-step procedure for classification prescribed in § 159a.15(c) does not apply to the classification of such foreign government information because E.O. 12356 states a presumption of damage to the national security in the event of unauthorized disclosure of such information. Therefore, foreign government information shall be classified at least Confidential, but higher whenever the damage criteria of § 159a.11 (b) or (c) are determined to be met.

(b) *Duration of Classification.* (1) Foreign government information shall not be assigned a date or event for automatic declassification unless specified or agreed to by the foreign entity.

(2) Foreign government information classified by the Department of Defense under this or previous regulations shall be protected for an indefinite period (see § 159a.77(e)).

§ 159a.76 Declassification.

(a) *Policy.* In considering the possibility of declassification of foreign government information, officials shall respect the intent of this regulation to protect foreign government information and confidential foreign sources.

(b) *Systematic Review.* When documents containing foreign government information are encountered during the systematic review process they shall be referred to the originating agency for a declassification determination. Consultation with the foreign originator through appropriate channels may be necessary before final action can be taken.

(c) *Mandatory Review.* Requests for mandatory review for declassification of foreign government information shall be processed and acted upon in accordance with the provisions of § 159a.26, except that foreign government information will be declassified only in accordance with the guidelines developed for such purpose and after necessary consultation with other DoD Components or government agencies with subject matter interest. When these guidelines cannot be applied to the foreign government information requested, or in the absence of such guidelines, consultation with the foreign originator through appropriate channels normally should be effected prior to final action taken on the request. When the responsibile DoD Component is knowledgeable of the foreign originator's view toward declassification or continued classification of the types of information requested, consultation with the foreign originator may not be necessary.

§ 159a.77 Marking.

(a) *Equivalent U.S. Classification Designations.* Except for the foreign security classification designation RESTRICTED, foreign classification designations, including those of international organizations of governments, that is, NATO, generally parallel U.S. classification designations. A table of equivalents is contained in Appendix A to this part.

(b) *Marking NATO Documents.* Classified documents originated by NATO, if not already marked with the appropriate classification in English, shall be so marked. Markings required under § 159a.34(c) shall not be placed on documents originated by NATO. Documents originated by NATO that are marked RESTRICTED shall be marked with the following additional notation: ''To be safeguarded in accordance with USSAN Instruction 1–69'' (see DoD Directive 5100.55).

(c) *Marking Other Foreign Government Documents.* (1) If the security classification designation of foreign government documents is shown in English, no other classification marking shall be applied. If the foreign classification designation is not shown in English, the equivalent overall U.S. classification designation (see Appendix A to this part) shall be marked conspicuously on the document. When foreign government documents are marked with a classification designation having no U.S. equivalent, as in the last column of Appendix A to this part, such documents shall be marked in accordance with paragraph (c)(2) of this section.

(2) Certain foreign governments use a fourth classification designation as shown in the last column of Appendix A to this part. Such designations equate to the foreign classification RESTRICTED. If the foreign government documents are marked with any of the classification designations listed in the last column of Appendix A to this part, no other classification marking shall be applied. In all such cases, the notation, ''This classified material is to be safeguarded in accordance with DoD 5200.1–R or DoD 5220.22–M,'' shall be shown on the face of the document.

(3) Other marking requirements prescribed by this Regulation for U.S. classified documents are not applicable to documents of foreign governments or international organizations of governments.

(d) *Marking of DoD Classification Determinations.* Foreign documents containing foreign government information not classified by the foreign government but provided to the Department of Defense in confidence shall be classified as prescribed in § 159a.75(a)(2) and marked with the appropriate U.S. classification.

(e) *Marking of Foreign Government Information in DoD Documents.* (1) Except where such markings would reveal that information is foreign government information when that fact must be concealed, or reveal a confidential source or relationship not otherwise evident

in the document or information, foreign government information incorporated in DoD documents shall be identified in a manner that ensures that such information is not declassified prematurely or made accessible to nationals of a third country without consent of the originator. This requirement may be satisfied by marking the face of the document ''FOREIGN GOVERNMENT INFORMATION,'' or with another marking that otherwise indicates that the information is foreign government information, and by including the appropriate identification in the portion or paragraph classification markings, for example, (NS) or (U.K.–C). All other markings prescribed by §159a.31(d) are applicable to these documents. In addition, DoD classified documents that contain extracts of NATO classified information shall bear a marking substantially as follows on the cover or first page: ''THIS DOCUMENT CONTAINS NATO CLASSIFIED INFORMATION.''

(2) When foreign RESTRICTED or NATO RESTRICTED information is included in an otherwise unclassified DoD document, the DoD document shall be marked CONFIDENTIAL. All requirements of §159a.31(d) apply to such documents. Portion markings on such a document include, for example ''(U),'' ''(NR),'' and ''(FRG–R).'' In addition, the appropriate caveat from paragraph (a) of this section, shall be included on the face of the document.

(3) The ''Classified by'' line of DoD documents containing only foreign government information normally shall be completed with the identity of the foreign government or international organization involved, for example, ''Classified by Government of Australia'' or ''Classfied by NATO,'' provided that other requirements of §159a.31(e) do not pertain to such documents.

(4) The ''Declassify on'' line of DoD documents containing foreign government information normally shall be completed with the notation ''Originating Agency's Determination Required'' or ''OADR'' (see §159a.36 and §159a.75(b)).

§159a.78 Protective measures.

(a) *NATO Classified Information.* NATO classified information shall be safeguarded in accordance with the provisions of DoD Directive 5100.55.

(b) *Other Foreign Government Information.* (1) Classified foreign government information other than NATO information shall be protected as is prescribed by this part for U.S. classified information of a comparable classification.

(2) Foreign government information, unless it is NATO information, that is marked under §159a.77(c)(2) or §159a.77(e)(2) shall be protected as U.S. CONFIDENTIAL, except that such information may be stored in locked filing cabinets, desks, or other similar closed spaces that will prevent access by unauthorized persons.

Subpart M—Special Access Programs

§159a.80 Policy.

It is the policy of the Department of Defense to use the security classification categories and the applicable sections of E.O. 12356 and its implementing ISOO Directive, to limit access to classified information on a ''need-to-know'' basis to personnel who have been determined to be trustworthy. It is further policy to apply the ''need-to-know'' principle in the regular system so that there will be no need to resort to formal Special Access Programs. Also, need-to-know control principles shall be applied within Special Access Programs. In this context, Special Access Programs may be created or continued only on specific showing that:

(a) Normal management and safeguarding procedures are not sufficient to limit ''need-to-know'' or access; and

(b) The number of persons who will need access will be reasonably small and commensurate with the objective of providing extra protection for the information invoved.

§159a.81 Establishment of special access programs.

(a) Procedures for the establishment of Special Access Programs involving NATO classified information are based

on international treaty requirements (see DoD Directive 5100.55).

(b) The policies and procedures for access to and dissemination of Restricted Data and Critical Nuclear Weapon Design Information are contained in DoD Directive 5210.2.

(c) Special Access Programs for foreign intelligence information under the cognizance of the Director of Central Intelligence, or those of the National Telecommunications and Information Systems Security Committee originate outside the Department of Defense. However, coordination with the DUSD(P) and the Component's central point of contact is necessary before the establishment or implementation of any such Programs by any DoD Component. The information required by § 159a.80(f)(1) will be provided.

(d) Excluding those Programs and that information specified in paragraphs (a)(1), (2), and (3) of this section, Special Access Programs shall be established within the Military Departments by:

(1) Submitting to the Secretary of the Department the information required under § 159a.80(f)(1).

(2) Obtaining written approval from the Secretary of the Department;

(3) Providing to the DUSD(P) notice of the approval; and

(4) Maintaining the information and rationale upon which approval was granted within the Military Department's central office.

(e) Excluding those Programs and that information in paragraphs (d)(1), (2), and (3) of this section, Special Access Programs that are desired to be established in any DoD Component other than the Military Departments shall be submitted with the information referred to in § 159a.80(f)(1) to the DUSD(P) for approval.

(f) Upon specific written notice to one of the appropriate DoD Special Access Program approval officials, receipt of their written concurrence, protective Special Access Program controls may be applied to a prospective Special Access Program for up to a 6-month period from the date of such notice. However, in all instances, the Program must be terminated as a prospective Special Access Program or formally approved as a Special Access Program by the end of the 6-month time period.

(g) Unless under DoD Directive S–5210.36[37], Special Access Programs which involve one or more DoD Components, or a DoD Component and a non-DoD activity, shall be covered by a written agreement which must document who has the principal security responsibility, who is the primary sponsor of the Program, and who is responsible for obtaining Special Access Program approval.

§ 159a.82 Review of special access programs.

(a) Excluding those Programs specified in § 159a.81 (a), (b), or (c), each Special Access Program shall be reviewed annually by the DoD Component responsible for establishment of the Program. To accommodate such reviews, DoD Components shall institute procedures to ensure the conduct of annual security inspections, with or without prior notice, and regularly scheduled audits by security, contract administration, and audit organizations. Also, Program managers shall ensure that Special Access Program activities have undergone a current review by legal counsel for compliance with law, executive order, regulation, and national policy. To accomplish such reviews, specially cleared pools of attorneys may be utilized, but in all cases legal counsel shall be provided with all information necessary to perform such reviews.

(b) Special Access Programs, excluding those specified in § 159a.81 (a), (b), or (c), or those required by treaty or international agreement, shall terminate automatically every 5 years unless reestablished in accordance with the procedures contained in § 159a.81.

§ 159a.83 Control and central office administration.

(a) Special Access Programs shall be controlled and managed in accordance with DoD Directive 5205.7[38]. Each DoD Component shall appoint a Special Access Program coordinator to establish and maintain a central office and to serve as a single point of contact for

[37] See footnote 13 to § 159a.33(j).

[38] See footnote 1 to § 159a.3.

information concerning the establishment and security administration of all Special Access Programs established by or existing in the Component. These officials shall report to the DUSD(P) on the status of DoD Special Access Programs within the Component to include:

(1) The establishment of a Special Access Program as required by §159a.81(d)(3); and

(2) Changes in Program status as required by §159a.85 (b) or (c).

(b) Officials serving as single points of contact, as well as members of their respective staffs and other persons providing support to Special Access Programs who require access to multiple sets of particularly sensitive information, shall be subject to a counterintelligence-scope polygraph examination periodically but not less than once every 5 years. Additionally, such testing will be subject to the limitations imposed by Congress. The program for each DoD Component, as well as requests for waiver, shall be submitted for approval by the DUSD(P).

§159a.84 Codewords and nicknames.

Excluding those Programs specified in §159a.81 (a), (b), and (c), each Special Access Program will be assigned a classified code word, or an unclassified nickname, or both. DoD Components other than Military Departments may request codewords and nicknames from the DUSD(P) individually or in block. If codewords or nicknames are obtained in block, however, the issuing Component shall promptly notify the DUSD(P) upon activitation and assignment.

§159a.85 Reporting of special access programs.

(a) *Report of Establishment.* Reports to the Secretary of the Military Department or the DUSD(P) required under §159a.81 for Special Access Programs shall include:

(1) The responsible department, agency, or DoD Component, including office identification;

(2) The codeword and/or nickname of the Program;

(3) The relationship, if any, to other Special Access Programs in the Department of Defense or other government agencies;

(4) The rationale for establishing the Special Access Program including the reason why normal management and safeguarding procedures for classified information are inadequate;

(5) The estimated number of persons granted special access in the responsible DoD Component; other DoD Components; other government agencies; contractors; and the total of such personnel;

(6) A summary statement pertaining to the Program security requirements with particular emphasis upon those personnel security requirements governing access to Program information;

(7) The date of Program establishment;

(8) The estimated number and approximate dollar value, if known, of carve-out contracts that will be or are required to support the Program; and

(9) The DoD Component official who is the point of contact (last name, first name, middle initial; position or title; mailing address; and telephone number).

(10) A security plan and appropriate security classification guide and notification that a proper DD Form 254, ''Contract Security Classification Specification,'' has been issued to contractors participating in the Program.

(b) *Annual Reports.* DoD Component annual reports from other than the Military Departments to the DUSD(P) shall be submitted not later than January 31 of each year, showing the changes in information provided under paragraph (a) of this section, as well as the date of last review. Annual reports shall reflect *actual* rather than *estimated* numbers of carve-out contracts and persons granted access and shall summarize the results of the inspections and audits required by §159a.82(a). Reports from the Military Departments which have approval authority will summarize the required reviews which have been conducted during the year by the central offices, to include details and numbers of carve-out contracts associated with approved Special Access Programs and their overall security posture and numbers

of approved Programs by type. Additionally, the Military Department Secretaries authorized to approve such Programs shall furnish a name listing, by unclassified nickname if practicable, or approved Special Access Programs under their cognizance, and they will report any changes to the listing as they occur pursuant to the notification requirements of §159a.81(d)(3), that is, additions, deletions, and corrections to the DUSD(P). The effective date of information in the annual reports shall be December 31.

(c) *Termination Reports.* The DUSD(P) shall be notified upon termination of a Special Access Program.

§159a.86 Accounting for special access programs.

Each of the central offices which must be identified in accordance with §159a.83(a) shall maintain a complete listing of currently approved DoD Special Access Programs which encompasses the information outlined in §159a.85(a). These listings shall be readily available to the DUSD(P) or his designated representatives.

§159a.87 Limitations on access.

Access to data reported under this subpart shall be limited to the DUSD(P) and the minimum number of properly indoctrinated staff necessary to perform the functions assigned the DUSD(P) herein. Access may not be granted to any other person for any purpose without the approval of the DoD Components sponsoring the Special Access Programs concerned.

§159a.88 "Carve-Out" contracts.

(a) The Secretaries of the Military Departments and the DUSD(P), or their designees, shall ensure that, in those Special Access Programs involving contractors, special access controls are made applicable by legally binding instruments.

(b) To the extent necessary for DIS to execute its security responsibilities with respect to Special Access Programs under its security cognizance, DIS personnel shall have access to all information relating to the administration of these Programs.

(c) Excluding those Programs specified in §159a.81(c), the use of ''carve-out'' contracts that relieve the DIS from inspection responsibility under the Defense Industrial Security Program is prohibited unless:

(1) Such contract supports a Special Access Program approved and administered under §159a.81;

(2) Mere knowledge of the existence of a contract or of its affiliation with the Special Access Program is classified information; and

(3) Carve-out status is approved for each contract by the Secretary of a Military Department, the Director, NSA, the DUSD(P), or their designees.

(d) Approval to establish a ''carve-out'' contract must be requested from the Secretary of a Military Department, or designee(s), the Director, NSA, or designee(s), or in the case of other DoD Components, from the DUSD(P). Approved ''carve-out'' contracts shall be assured the support necessary for the requisite protection of the classified information involved. The support shall be specified through a system of controls that shall provide for:

(1) A written security plan, oral waivers of which are prohibited except in critical situations that must be documented as soon as possible after the fact.

NOTE: The plan must identify that DD Forms 254 have been distributed to the Defense Investigative Service as outlined in DoD Directive 5205.7.

(2) Professional security personnel at the sponsoring DoD Component performing security inspections at each contractor's facility which shall be conducted, at a minimum, with the frequency prescribed by paragraph 4–103 of DoD 5220.22–R;

(3) ''Carve-out'' contracting procedures;

(4) A central office of record; and

(5) An official to be the single point of contact for security control and administration. DoD Components other than the Military Departments and NSA shall submit such appropriate rationale and security plan along with requests for approval to the DUSD(P).

(e) An annual inventory of carve-out contracts shall be conducted by each DoD Component which participates in Special Access Programs.

(f) This subsection relates back to the date of execution for each contract to which carve-out contracting techniques are applied. The carve-out status of any contract expires upon termination of the Special Access Program which it supports.

§ 159a.89 Oversight reviews.

(a) DUSD(P) shall conduct oversight reviews, as required, to determine compliance with this subpart.

(b) Pursuant to statutory authority, the Inspector General, Department of Defense, shall conduct oversight of Special Access Programs.

Subpart N—Program Management

§ 159a.91 Executive branch oversight and policy direction.

(a) *National Security Council.* Pursuant to the provisions of E.O. 12356, the NSC shall provide overall policy direction for the Information Security Program.

(b) *Administrator of General Services.* The Administrator of General Services is responsible for implementing and monitoring the Information Security Program established under E.O. 12356. In accordance with E.O. 12356, the Administrator delegates the implementation and monitorship functions of the Program to the Director of the ISOO.

(c) *Information Security Oversight Office*—(1) *Composition.* The ISOO has a full-time director appointed by the Administrator of General Services with approval of the President. The Director has the authority to appoint a staff for the office.

(2) *Functions.* The Director of the ISOO is charged with the following principal functions that pertain to the Department of Defense:

(i) Oversee DoD actions to ensure compliance with E.O. 12356 implementing directives, for example, the ISOO Directive No. 1 and this part;

(ii) Consider and take action on complaints and suggestions from persons within or outside the government with respect to the administration of the Information Security Program;

(iii) Report annually to the President through the NSC on the implementation of E.O. 12356;

(iv) Review this Regulation and DoD guidelines for systematic declassification review; and

(v) Conduct on-site reviews of the Information Security Program of each DoD Component that generates or handles classified information.

(3) *Information Requests.* The Director of the ISOO is authorized to request information or material concerning the Department of Defense, as needed by the ISOO in carrying out its functions.

(4) *Coordination.* Heads of DoD Components shall ensure that any significant requirements levied directly on the Component by the ISOO are brought to the attention of the Director of Security Plans and Programs, ODUSD(P).

§ 159a.92 Department of Defense.

(a) *Management Responsibility.* (1) The DUSD(P) is the Senior DoD Information Security Authority having DoD-wide authority and responsibility to ensure effective and uniform compliance with and implementation of E.O. 12356 and its implementing ISOO Directive No. 1. As such, the DUSD(P) shall have primary responsibility for providing guidance, oversight and approval of policy and procedures governing the DoD Information Security Program. The DUSD(P) or his designee may approve waivers or exceptions to the provisions of this part to the extent such action is consistent with E.O. 12356 and ISOO Directive No. 1.

(2) The heads of DoD Components may approve waivers to the provisions of this part only as specifically provided for herein.

(3) The Director, NSA/Chief, Central Security Service, under 32 CFR part 159, is authorized to impose special requirements with respect to the marking, reproduction, distribution, accounting, and protection of and access to classified cryptologic information. In this regard, the Director, NSA, may approve waivers or exceptions to these special requirements. Except as provided in §159a.6 the authority to lower any COMSEC security standards rests with the Secretary of Defense. Requests for approval of such waivers or exceptions to established COMSEC security standards which, if adopted, will

have the effect of lowering such standards, shall be submitted to the DUSD(P) for approval by the Secretary of Defense.

§ 159a.93 DoD components.

(a) *General.* The head of each DoD Component shall establish and maintain an Information Security Program designed to ensure compliance with the provisions of this part throughout the Component.

(b) *Military Departments.* In accordance with 32 CFR part 159 the Secretary of each Military Department shall designate a Senior Information Security Authority who shall be responsible for complying with and implementing this part within the Department.

(c) *Other Components.* In accordance with 32 CFR part 159, the head of each other DoD Component shall designate a Senior Information Security Authority who shall be responsible for complying with and implementing this Regulation within their respective Component.

(d) *Program Monitorship.* The Senior Information Security Authorities designated under paragraphs (b) and (c) of this section, are responsible within their respective jurisdictions for monitoring, inspecting with or without prior announcement, and reporting on the status of administration of the DoD Information Security Program at all levels of activity under their cognizance.

(e) *Field Program Management.* (1) Throughout the Department of Defense, the head of each activity shall appoint, in writing, an official to serve as security manager for the activity. This official shall be responsible for the administration of an effective Information Security Program in that activity with particular emphasis on security education and training, assignment of proper classifications, downgrading and declassification, safeguarding, and monitorship, to include sampling classified documents for the purpose of assuring compliance with this part.

(2) Activity heads shall ensure that officials appointed as security managers either possess, or obtain within a reasonable time after appointment, knowledge of and training in the Information Security Program commensurate with the needs of their positions. The Director of Security Plans and Programs, ODUSD(P) shall, with the assistance of the Director, Defense Security Institute, develop minimum standards for training of activity security managers. Such training should result in appropriate certifications to be recorded in the personnel files of the individuals involved.

(3) Activity heads shall ensure that officials appointed as security managers are authorized direct and ready access to the appointing official on matters concerning the Information Security Program. They also shall provide sufficient resources of time, staff, and funds to permit accomplishment of the security manager's responsibilities, to include meaningful oversight of the Information Security Program at all levels of the activity.

§ 159a.94 Information requirements.

(a) *Information Requirements.* DoD Components shall submit on a fiscal year basis a consolidated report concerning the Information Security Program of the Component on SF 311, ''Agency Information Security Program Data,'' to reach the ODUSD(P) by October 20 of each year. SF 311 shall be completed in accordance with the instructions thereon and augmenting instructions issued by the ODUSD(P). The ODUSD(P) shall submit the DoD report (SF 311) to the ISOO by October 31 of each year. Interagency Report Control Number 0230–GSA–AN applies to this information collection system as well as to that contained in § 159a.12.

§ 159a.95 Defense Information Security Committee.

(a) *Purpose.* The Defense Information Security Committee (DISC) is established to advise and assist the DUSD(P) and the Director, Security Plans and Programs (ODUSD(P)) in the formulation of DoD Information Security Program policy and procedures.

(b) *Direction and Membership.* The DISC shall meet at the call of the DUSD(P) or the Director, Security Plans and Programs. It is comprised of the DUSD(P) as Chairman; the Director, Security Plans and Programs, as Vice Chairman; and the senior officials

(designated in accordance with section E.3.a., DoD Directive 5200.1,[39] or their representatives) responsible for directing and administering the Information Security Program of the OJCS, the Departments of the Army, Navy, and Air Force, the Defense Intelligence Agency, the Defense Nuclear Agency, the National Security Agency, and the Defense Investigative Service. Other DoD Components may be invited to attend meetings of particular interest to them.

Subpart O—Administrative Sanctions

§ 159a.97 Individual responsibility.

All personnel, civilian or military, of the Department of Defense are responsible individually for complying with the provisions of this part.

§ 159a.98 Violations subject to sanctions.

(a) DoD Military and civilian personnel are subject to administrative sanctions if they:

(1) Knowingly and willfully classify or continue the classification of information in violation of E.O. 12356, any implementing issuances, or this part.

(2) Knowingly, willfully, or negligently disclose to unauthorized persons information properly classified under E.O. 12356 or prior orders; or

(3) Knowingly and willfully violate any other provision of E.O. 12356, any implementing issuances or this part.

(b) Sanctions include but are not limited to a warning notice, reprimand, termination of classification authority, suspension without pay, forfeiture of pay, removal or discharge, and will be imposed upon any person, regardless of office or level of employment, who is responsible for a violation specified under this paragraph as determined appropriate under applicable law and DoD regulations. Nothing in this part prohibits or limits action under the Uniform Code of Military Justice based upon violations of that Code.

§ 159a.99 Corrective action.

The Secretary of Defense, the Secretaries of the Military Departments, and the heads of other DoD Components shall ensure that appropriate and prompt corrective action is taken whenever a violation under §159a.98(a) occurs or repeated administrative discrepancies or repeated disregard of requirements of this Regulation occur (see §159a.100). Commanders and supervisors, in consultation with appropriate legal counsel, shall utilize all appropriate criminal, civil, and administative enforcement remedies against employees who violate the law and security requirements as set forth in this part and other pertinent DoD issuances.

§ 159a.100 Administrative discrepancies.

Repeated administrative discrepancies in the marking and handling of classified information and material such as failure to show classification authority; failure to apply internal classification markings; failure to adhere to the requirements of this part that pertain to dissemination, storage, accountability, and destruction, and that are determined not to constitute a violation under §159a.98(a) may be grounds for adverse administrative action including warning, admonition, reprimand or termination of classification authority as determined appropriate under applicable policies and procedures.

§ 159a.101 Reporting violations.

(a) Whenever a violation under §159a.98(a)(2) occurs, the Director of Counterintelligence and Investigative Programs, ODUSD(P) shall be informed of the date and general nature of the occurrence including the relevent parts of this part, the sanctions imposed, and the corrective action taken. Whenever a violation under §159a.98(a) (1) or (3) occurs, the Director of Security Plans and Programs, OSUSD(P) shall be provided the same information. Notification of such violations shall be furnished to the Director of the ISOO in accordance with §5.4(d) of E.O. 12356 by the ODUSD(P).

(b) Any action resulting in unauthorized disclosure of properly classified information that constitutes a violation of the criminal statutes and evidence reflected in classified information of

[39] See footnote 1 to §159a.3

possible violations of Federal criminal law by a DoD employee and of possible violations by any other person of those Federal criminal laws specified in guidelines adopted by the Attorney General shall be the subject of a report processed in accordance with DoD Directive 5210.50 and DoD Instruction 5240.4.

(c) Any action reported under paragraph (b) of this section, shall be reported to the Attorney General by the General Counsel, Department of Defense.

(d) Reports shall be made to appropriate counterintelligence, investigative, and personnel security authorities concerning any employee who is known to have been responsible for repeated security violations over a period of a year, for appropriate evaluation, including readjudication of the employee's security clearance.

APPENDIX A TO PART 159A—EQUIVALENT FOREIGN AND INTERNATIONAL PACT ORGANIZATION SECURITY CLASSIFICATIONS

Country	Top Secret	Secret	Confidential	
Argentina	Estrictamente Secreto	Secreto	Confidencial	Reservado.
Australia	Top Secret	Secret	Confidential	
Austria	Streng Geheim	Geheim	Verschuluss	
Belgium:				
French	Tres Secret	Secret	Confidentiel Restreints	Difusion.
Flemish	Zeer Geheim	Geheim	Vertrouwelijk Verspreiding	Bepertke.
Bolivia	Syoersecreto or Muy Secreto	Secreto	Confidencial	Resedrvado.
Brazil	Ultra Secreto	Secreto	Confidencial	Reservado.
Cambodia	Tres Secret	Secret	Secret/Confidential	
Canada	Top Secret	Secret	Confidential	Restricted.
Chile	Secreto	Secreto	Reservado	Reservado.
Columbia	Ultrasecreto	Secreto	Reservado Restringido	Confidencial.
Costa Rica	Alto Secreto	Secreto	Confidencial	
Denmark	Hojst Himmiligt	Himmiligt	Fortroligt	Til Tjenestebrug.
Ecuador	Secretisimo	Secreto	Confidencial	Reservado.
El Salvador	Ultra Secreto	Secreto	Confidencial	Reservado.
Ethiopia	Yemlaz Birtou Mistir	Kilkil		
Finland	Erittain Salainen	Salainen		
France	Tres Secret	Secret Defense	Confidentiel Defense Restreinte.	Diffusion.
Germany	Streng Geheim	Geheim	Va-Vertraulich	
Greece	Akpre Anopphton	Anopphton	Emilieteytikon Xpheere	Mepinpiemenhe.
Guatemala	Alto Secreto	Secreto	Confidencial	Reservado.
Haiti		Secret	Confidential	
Honduras	Super Secreto	Secreto	Confidencial	Reservado.
Hong Kong	Top Secret	Secret	Confidential	Restricted.
Hungary	Szigoruan Titkos	Titkos	Bizalmas	
India	Top Secret	Secret	Confidential	Restricted.
Indonesia	Sangat Rahasia	Rahasia	Terbatas	
Iran	Bekoli Serri	Serri	Kheili Mahramaneh	Mahramaneh.
Iraq	(Absolutely secret)	(Secret)		(Limited).
Ireland Gaelic	Top Secret An-Sicreideach	Secret Sicreideach	Confidential Runda	Restricted Srianta.
Israel	Sodi Beyoter	Sodi	Shamur	Mugbal.
Italy	Segretissimo	Segreto	Riservatissimo	Riservato.
Japan	Kimitsu	Gokuhi	Hi Bugaihi	Toriatsukaichui.
Jordan	Maktum Jiddan	Maktum	Sirri	Mahdud.
Korea				
Laos	Tres Secret	Secret	Secret/Confidentiel Restreinte	Difusion.
Lebanon	Tres Secret	Secret	Confidentiel	
Mexico	Alto Secreto	Secreto	Confidencial	Restringido.
Netherlands	Zeer Geheim	Geheim	Confidentieel or Vertrouwelijk	Dienstgeheim.
New Zealand	Top Secret	Secret	Condifential	Dienstgeheim.
Nicaragua	Alto Secreto	Secreto	Confidencial	Reservado.
Norway	Strengt Hemmelig	Hemmelig	Konfideneielt	Begrenset.
Pakistan	Top Secret	Secret	Confidential	Restricted.
Paraguay	Secreto	Secreto	Confidencial	Reservado.
Peru	Estrictamente Secreto	Secreto	Condifencial	Reservado.
Philippines	Top Secret	Secret	Confidential	Restricted.
Portugal	Muito Secreto	Secreto	Confidencial	Reservado.
Spain	Maximo Secreto	Secreto	Confidencial Limitada	Diffussion.
Sweden (Red Borders).	Hemlig	Hemlig	Hemlig	
Switzerland	(1)	(1)	(1)	
French	Secret	Secret	Secret Exclusive Du	Reserve A L'Usage.

APPENDIX A TO PART 159A—EQUIVALENT FOREIGN AND INTERNATIONAL PACT ORGANIZATION SECURITY CLASSIFICATIONS—Continued

Country	Top Secret	Secret	Confidential	
German	Streng Geheim	Geheim	Vertraulich Lichen Gebrauch	Nur Fur Dienst-
Italian	Segreto	Segreto	Segreto Di Servizio	Ad Exclusive Uso.
Thailand	Lup Tisud	Lup Maag	Lup	Pok Pid.
Turkey	Cok Gizli	Gizli	Ozel	Hizmete Ozel.
Union of South Africa:				
English	Top Secret	Secret	Confidential	Restricted.
Afrikaana	Uiters Geheim	Geheim	Vertroulik	Reperk.
United Arab Republic (Egypt).	Top Secret	Very Secret	Secret	Official.

[1] Three languages. TOP SECRET has a registration number to distinguish from SECRET and CONFIDENTIAL.

Country	TOP SECRET	SECRET	CONFIDENTIAL	
United Kingdom	TOP SECRET	SECRET	CONFIDENTIAL	RESTRICTED
Uruguay	ULTRA SECRETO	SECRETO	CONFIDENCIAL	RESERVADO
USSR	СОВЕРШЕННО СЕКРЕТНО	СЕКРЕТНО	НЕ ПОДЛЕЖАЩИЙ ОГЛАШЕНИЮ	ДЛЯ СЛУЖЕБНОГО ПОЛЬЗОВАНИЯ
Viet Nam French	TRES SECRET	SECRET DEFENSE	CONFIDENTIEL DEFENSE	DIFFUSION RESTREINTE
Vietnamese	TỐI-MẬT	MẬT	KIN	TU MẬT
INTERNATIONAL ORGANIZATION	TOP SECRET	SECRET	CONFIDENTIAL	(SEE CHAPTER XI)
NATO	COSMIC TOP SECRET	NATO SECRET	NATO CONFIDENTIAL	NATO RESTRICTED

NOTES:

In all instances foreign security classification systems are not exactly parallel to the U.S. system and exact equivalent classifications cannot be stated. The classifications given above represent the nearest comparable designations that are used to signify degrees of protection and control similar to those prescribed for the equivalent U.S. classifications.

"ATOMAL" information is an exclusive designation used by NATO to identify "Restricted Data" or "Formerly Restricted Data" information released by the U.S. Government to NATO.

[54 FR 26959, June 27, 1989, as amended at 54 FR 31334, July 28, 1989]

APPENDIX B TO PART 159a—GENERAL ACCOUNTING OFFICE OFFICIALS AUTHORIZED TO CERTIFY SECURITY CLEARANCES (SEE § 159a.53(b)(3))

The Comptroller General, Deputy Comptroller General and Assistant Comptroller General and Assistants to the Comptroller General

The General Counsel and Deputy General Counsel

The Director and Deputy Director, Personnel; the Security Officer

The Director and Deputy Director, Office of Internal Review

The Director and Assistants to the Director of the Office of Program Planning and the Office of Policy

The Director and Deputy Directors of the Community and Economic Development Division

The Director, and Deputy Directors, Associate Directors, Deputy Associate Directors, Senior Group Directors, and the Assistant to the Director for Planning and Administration of the Energy and Minerals Division

The Director, Deputy Directors, Associate Directors and Division Personnel Security Officer of the Human Resources Division

The Directors, Deputy Directors, and Associate Directors, of the following Divisions:

Claims
Field Operations
Financial and General Management Studies
General Government
International
Logistics and Communications
Procurement and Systems Acquisition
Program Analysis Division

Directors and Managers of International Division Overseas Offices as follows:

Director European Branch, Frankfurt, Germany
Director Far East Branch, Honolulu, Hawaii
Manager, Sub Office, Bangkok, Thailand

Regional Managers and Assistsant Regional Managers of the Field Operations Division's Regional Offices as follows:

Atlanta, Georgia
Boston, Massachusetts
Chicago, Illinois
Cincinnati, Ohio
Dallas, Texas
Denver, Colorado
Detroit, Michigan
Kansas City, Missouri
Los Angeles, California
New York, New York
Norfolk, Virginia
Philadelphia, Pennsylvania
San Francisco, California
Seattle, Washington
Washington, D.C.

APPENDIX C TO PART 159a—INSTRUCTIONS GOVERNING USE OF CODE WORDS, NICKNAMES, AND EXERCISE TERMS (SEE § 159a.54(j))

1. Definitions

a. *Using Component.* The DoD Component to which a code word is allocated for use, and which assigns to the word a classified meaning, or which originates nicknames and exercise terms using the procedure established by the Joint Chiefs of Staff.

b. *Code Word.* A single word selected from those listed in Joint Army-Navy-Air Force Publication (JANAP) 299 and later volumes, and assigned a classified meaning by appropriate authority to insure proper security concerning intentions, and to safeguard information pertaining to actual military plans or operations classified as Confidential or higher. A code word shall not be assigned to test, drill or exercise activities. A code word is placed in one of three categories:

(1) *Available.* Allocated to the using component. Available code words *individually* will be unclassified until placed in the active category.

(2) *Active.* Assigned a classified meaning and current.

(3) *Canceled.* Formerly active, but discontinued due to compromise, suspected compromise, cessation, or completion of the operation to which the code word pertained. Canceled code words *individually* will be unclassified and remain so until returned to the active category.

c. *Nickname.* A combination of two separate unclassified words which is assigned an unclassified meaning and is employed only for unclassified administrative, morale, or public information purposes.

d. *Exercise Term.* A combination of two separate unclassified words, normally unclassified, used exclusively to designate a test, drill, or exercise. An exercise term is employed to preclude the possibility of confusing exercise directions with actual operations directives.

2. Policy and Procedure

a. *Code Words.* The Joint Chiefs of Staff are responsible for allocating words or blocks of code words from JANAP 299 to DoD Components. DoD Components may request allocation of such code words as required and may reallocate available code words within their organizations, in accordance with individual policies and procedure, subject to applicable rules set forth herein.

(1) A permanent record of all code words shall be maintained by the Joint Chiefs of Staff.

(2) The using Component shall account for available code words and maintain a record of each active code word. Upon being canceled, the using component shall maintain

the record for 2 years; thence the record of each code word may be disposed of in accordance with current practices, and the code word returned to the available inventory.

b. *Nicknames*

(1) Nicknames may be assigned to actual events, projects, movement of forces, or other nonexercise activities involving elements of information of any classification category, but the nickname, the description or meaning it represents, and the relationship of the nickname and its meaning must be unclassified. A nickname is not designed to achieve a security objective.

(2) Nicknames, improperly selected, can be counterproductive. A nickname must be chosen with sufficient care to ensure that it does not:

(a) Express a degree of bellicosity inconsistent with traditional American ideals or current foreign policy;

(b) Convey connotations offensive to good taste or derogatory to a particular group, sect, or creed; or,

(c) Convey connotations offensive to our allies or other Free World nations.

(3) The following shall not be used as nicknames:

(a) Any two-word combination voice call sign found in JANAP 119 or ACP 110. (However, single words in JANAP 119 or ACP 110 may be used as part of a nickname if the first word of the nickname does not appear in JANAP 299 and later volumes.)

(b) Combination of words including word ''project,'' ''exercise,'' or ''operation.'' (The word ''project'' often is used as the first or second word with an unclassified nickname originating outside the Department of Defense.)

(c) Words that may be used correctly either as a single word or as two words, such as ''moonlight.''

(d) Exotic words, trite expressions, or well-known commercial trademarks.

(4) The Joint Chiefs of Staff shall:

(a) Establish a procedure by which nicknames may be authorized for use by DoD Components.

(b) Prescribe a method for the using Components to report nicknames used.

(5) The heads of DoD Components shall:

(a) Establish controls within their Components for the assignment of nicknames authorized under subparagraph 2.b.(4)(a), above.

(b) Under the procedures established, advise the Joint Chiefs of Staff of nicknames as they are assigned.

c. *Exercise Term*

(1) Unclassified exercise terms may be assigned only to tests, drills, or exercises for the purpose of emphasizing that the event is a test, drill, or exercise and not an actual operation. However, the description or meaning it represents, and the relationship of the exercise term and its meaning can be classified or unclassified. A classified exercise term is not authorized.

(2) Selection of exercise terms will follow the same guidance as contained in subparagraphs 2.b.(2) and (3), above.

(3) The Joint Chiefs of Staff shall:

(a) Establish a procedure by which exercise terms may be authorized for use by DoD Components.

(b) Prescribe a method for using Components to report exercise terms used.

(4) The heads of DoD Components shall:

(a) Establish controls within their Component for the assignment of exercise terms authorized under subparagraph 2.c.(3), above.

(b) Under the procedures established, advise the Joint Chiefs of Staff of exercise terms as they are assigned.

3. Assignment of Classified Meanings to Code Words

a. The DoD Component responsible for the development of a plan or the execution of an operation shall be responsible for determining whether to assign a code word.

b. Code words shall be activated for the following purposes only:

(1) To designate a classified military plan or operation;

(2) To designate classified geographic locations in conjunction with plans or operations referred to in subparagraph 3.b.(1), above; or,

(3) To cancel intentions in discussions and messages or other documents pertaining to plans, operations, or geographic locations referred to in subparagraphs 3.b.(1) and (2), above.

c. The using Component shall assign to a code word a specific meaning classified Secret or Confidential. Code words shall not be used to cover unclassified meanings. The assigned meaning need not in all cases be classified as high as the overall classification assigned to the plan or operation. Top Secret code words may be issued only with DUSD(P) or DoD Component head approval.

d. Code words shall be selected by each using Component in such manner that the word used does not suggest the nature of its meaning.

e. A code word shall not be used repeatedly for similar purposes; that is, if the initial phase of an operation is designated ''Meaning,'' succeeding phases shall not be designated ''Meaning II'' and ''Meaning III,'' but should have different code words.

f. Each DoD Component shall establish policies and procedures for the control and assignment of classified meanings to code words, subject to applicable rules set forth herein.

4. Notice of Assignment, Dissemination, and Cancelation of Code Words and Meanings

a. The using Component shall promptly notify the Joint Chiefs of Staff when a code

word is made active, indicating the word, and its classification. Similar notice shall be made when any changes occur, such as the substitution of a new word for one previously placed in use.

b. The using Component is responsible for further dissemination of active code words and meanings to all concerned activities, to include classification of each.

c. The using Component is responsible for notifying the Joint Chiefs of Staff of canceled code words. This cancellation report is considered final action, and no further reporting or accounting of the status of the canceled code word will be required.

5. Classification and Downgrading Instructions

a. During the development of a plan, or the planning of an operation by the headquarters of the using Component, the code word and its meaning shall have the same classification. When dissemination of the plan to other DoD Components or to subordinate echelons of the using Component is required, the using Component may downgrade the code words assigned below the classification assigned to their meanings in order to facilitate additional planning implementation, and execution by such other Components or echelons, but code words shall, at a minimum, be classified Confidential.

b. A code word which is replaced by another code word due to a compromise or suspected compromise, or for any other reason, shall be canceled, and classified Confidential for a period of 2 years, after which the code word will become unclassified.

c. When a plan or operation is discontinued or completed, and is not replaced by a similar plan or operation but the meaning cannot be declassified, the code word assigned thereto shall be canceled and classified Confidential for a period of 2 years, or until the meaning is declassified, whichever is sooner, after which the code word will become unclassified.

d. In every case, whenever a code word is referred to in documents, the security classification of the code word shall be placed in parentheses immediately following the code word, for example, ''Label (C).''

e. When the meaning of a code word no longer requires a classification, the using Component shall declassify the meaning and the code word and return the code word to the available inventory.

6. Security Practices

a. The meaning of a code word may be used in a message or other document, together with the code word, only when it is essential to do so. Active code words may be used in correspondence or other documents forwarded to addresses who may or may not have knowledge of the meaning. If the context of a document contains detailed instructions or similar information which indicates the purpose or nature of the related meaning, the active code word shall not be used.

b. In handling correspondence pertaining to active code words, care shall be used to avoid bringing the code words and their meanings together. They should be handled in separate card files, catalogs, indexes, or lists, enveloped separately, and dispatched at different times so they do not travel through mail or courier channels together.

c. Code words shall not be used for addresses, return addresses, shipping designators, file indicators, call signs, identification signals, or for other similar purposes.

7. Former Words

All code words formerly categorized as ''inactive'' or ''obsolete'' shall be placed in the current canceled category and classified Confidential. Unless otherwise restricted, all code words formerly categorized as ''canceled'' or ''available'' shall be individually declassified. All records associated with such code words may be disposed of in accordance with current practices, provided such records have been retained at least 2 years after the code words were placed in the former categories of ''inactive,'' ''obsolete,'' or ''canceled.''

8. Non-DoD Words

Nicknames or code words originating outside of the Department of Defense that are jointly used by the originating organization and the Department of Defense shall be registered with the DUSD(P) to prevent confusion with DoD-originated words.

APPENDIX D TO PART 159a—FEDERAL AVIATION ADMINISTRATION AIR TRANSPORTATION, SECURITY FIELD OFFICES (SEE §159a.59(c)(1)(i))

City	*State*
Anchorage	Alaska
Atlanta	Georgia
Baltimore	Maryland
Boston	Massachusetts
Chicago (O'Hare)	Illinois
Cleveland	Ohio
Dallas	Texas
Denver	Colorado
Detroit	Michigan
Honolulu	Hawaii
Houston	Texas
Kansas City	Missouri
Las Vegas	Nevada
Los Angeles	California
Miami	Florida
Minneapolis	Minnesota
Newark	New Jersey
New Orleans	Louisiana
New York (John F. Kennedy)	New York
New York (La Guardia)	New York
Philadelphia	Pennsylvania
Pittsburgh	Pennsylvania
Portland	Oregon

City	State
St. Louis	Missouri
San Antonio	Texas
San Diego	California
San Francisco	California
San Juan	Puerto Rico
Seattle	Washington
Tampa	Florida
Tucson	Arizona
Washington (Dulles)	Washington, DC
Washington (National)	Washington, DC

APPENDIX E TO PART 159a—TRANSPORTATION PLAN (SEE § 159a.57(e))

The provisions of § 159a.57(e) of this part require that transmission instructions or a separate transportation plan be included with any contract, agreement or other arrangement involving the release of classified material to foreign entities. The transportation plan is to be submitted to and approved by applicable DoD authorities. As a minimum, the transportation plan shall include the following provisions:

a. A description of the classified material together with a brief narrative as to where and under what circumstances transfer of custody will occur;

b. Identification, by name or title, of the designated representative of the foreign recipient government or international organization who will receipt for and assume security responsibility for the U.S. classified material (person(s) so identified must be cleared for access to the level of the classified material to be shipped);

c. Identification and specific location of delivery points and any transfer points;

d. Identification of commercial carriers and freight forwarders or transportation agents who will be involved in the shipping process, the extent of their involvement, and their security clearance status;

e. Identification of any storage or processing facilities to be used and, relative thereto, certification that such facilities are authorized by competent government authority to receive, store, or process the level of classified material to be shipped;

f. When applicable, the identification, by name or title, of couriers and escorts to be used and details as to their responsibilities and security clearance status;

g. Description of shipping methods to be used as authorized by the provisions of subpart I, together with the identification of carriers (foreign and domestic);

h. In those cases when it is anticipated that the U.S. classified material or parts thereof may be returned to the United States for repair, service, modification, or other reasons, the plan must require that shipment shall be via a carrier of U.S. or recipient government registry, handled only by authorized personnel, and that the applicable Military Department (for foreign military sales (FMS)) or Defense Investigative Service (for commercial sales) will be given advance notification of estimated time and place of arrival and will be consulted concerning inland shipment;

i. The plan shall require the recipient government or international organization to examine shipping documents upon receipt of the classified material in its own territory and advise the responsible Military Department in the case of FMS, or Defense Investigative Service in the case of commercial sales, if the material has been transferred enroute to any carrier not authorized by the transportation plan; and

j. The recipient government or international organization also will be required to inform the responsible Military Department or the Defense Investigative Service promptly and fully of any known or suspected compromise of U.S. classified material while such material is in its custody or under its cognizance during shipment.